~~SECRET~~

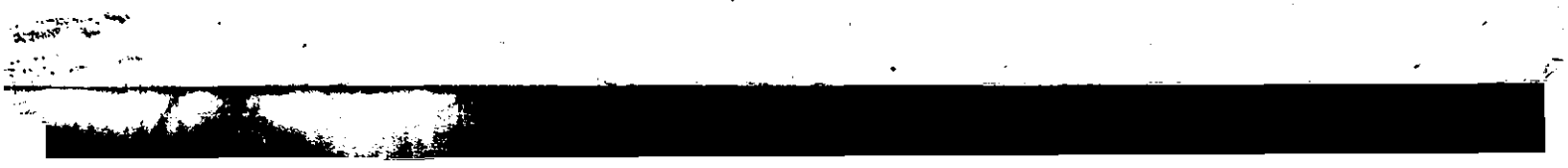
Copy No. 152

S. I. COURSE

SOLUTIONS

Vol. II

1942



S.I. COURSE

S E C T I O N IV

POLY-ALPHABETIC CIPHERS

1. The words A TIDE IN which have been found in the key suggest the Shakespearean lines THERE IS A TIDE IN THE AFFAIRS OF MEN WHICH TAKEN AT THE FLOOD..... When this is tested, it is found to be correct since it produces sense for the message.

Key:	T	H	E	R	E	I	S	A	T	I	D	E	I	N	T	H	E	A	F	F		
Message:	H	O	S	T	I	L	E	X	T	A	N	K	S	X	R	E	P	O	R	T		
	A	I	R	S	O	F	H	E	N	W	H	I	C	H	T	A	K	E	N			
	E	D	X	V	I	C	I	N	I	T	Y	X	B	E	D	F	O	R	D			

2. It is known that both Plain and Cipher components consist of the following sequence

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
W	A	L	T	D	I	S	N	E	Y	U	M	B	O	C	F	G	H	J	K	P	Q	R	V	X	Z

and that TRUNK probably occurs in the key or in the message or in both. Two methods of approach, therefore, are now possible, (i) "stencil-search", (ii) "drag" with numerical representation of letters (e.g. TRUNK is 3 22 10 7 19). Either method should reveal the following three possible positions for the word TRUNK.

Cipher		E	N	J	C	Z					M	Z	A	F	T					I	W	V	Q	N
Text	I	T	R	U	N	K		II		T	R	U	N	K		III		T	R	U	N	K			
Text		I	M	E	N	S					E	T	H	E	U					L	D	O	C	C

SPECIMENS is one of the few words which will fit I, II it is at present difficult to extend, III appears to require WOULD (or SHOULD) OCCUPY (or OCCUR). In this last case we obtain the following result which looks promising:

Cipher	T	D	J	I	W	V	Q	N	R	L	W
Text	T	H	E	T	R	U	N	K	B	E	H
Text	W	O	U	L	D	O	C	C	U	P	Y

Once a start has been made it is not too difficult to play off the one text against the other, especially as it soon becomes apparent that both message and key are rhyming verse dealing with the same subject. If, however, it is found impossible to proceed, a guess will have to be made at another probable word, and from consideration of the key-phrase and the probable word already given, we might well try ELEPHANT.

It must be remembered that as this is a Vigenère encipherment, it is impossible to establish which words occur in the message and which in the key with the result that, when several disconnected portions of text have been solved, it may not be possible to decide immediately how they are interrelated. e.g. In this present example with the two separate portions

T R U N K		T H E T R U N K B E H
	and	
S P E C I M E N S		W O U L D O C C U P Y

it is at that stage impossible to say of the word SPECIMENS whether it is in the same text as WOULD OCCUPY or in the same text as THE TRUNK BEH.

The key and message are as follows:-

A T A I L B E H I N D A T R U N K I N F R O N T
I F Y O U F O R S P E C I M E N S S H O U L D H

C O M P L E T E T H E U S U A L E L E P H A N T S T
U N T W I T H T R U N K S B E H I N D A N D T A I L

O P T H E T A I L I N F R O N T T H E T R U N K B E
S I N F R O N T T H A T H U N T W O U L D O C C U P

H I N D I S W H A T Y O U V E R Y S E I D O M F I N
Y Y O U L O N G S E M I C O L O N T H E F O R C E O

D E N D O F F I R S T V E R S E
F H A B I T I S S O S T R O N G

3. The two components are known to be

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

In order to construct the table for the stencil-search method, the cipher text is written out and each letter is then used as the starting point for the known cipher component. The plain component is then written down at the left as an index, starting at the top line of the table, because Beaufort encipherment has been employed. Stencils, which must of course be based on the plain component, are cut for probable message words, e.g. COMPROMISED, CIPHER, CHANGE.

Below is shown one result of trying CIPHER.

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

The message and key are now built up in the usual way by playing off one against the other, and the solution is found to be as follows:-

Message: O U R P R E S E N T C I P H E R I S B E

Key: H I S F A C E I S B L A C K H I S C R O

L I E V E D T O B E C O M P R O M I S E D S T O P

W N M O U S T A C H E S A N D B A C K O F T H E H

C H A N G E K E Y D A I L Y U S I N G I N Y O U R

E A D A R E C R I M S O N H I S R U M P I S B R I

M E S S A G E S R E S E R V E C I P H E R Q T W E L V E

G H T Y E L L O W H I S B A C K I S O L I V E G R E E N

4a. The cipher text is written out and each letter is then taken as the starting point for the cipher component which is known to be the normal alphabetical sequence. The diagonals are inspected for clear text and it is found that a progression key of 2 has been used. (Note, however, that all 26 possible cipher alphabets have been used, so that the progression key is actually 2 2 2 2 2 2 2 2 2 2 2 2 2 3 2 2 2 2 2 2 2 2 2 2 2 2 1).

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

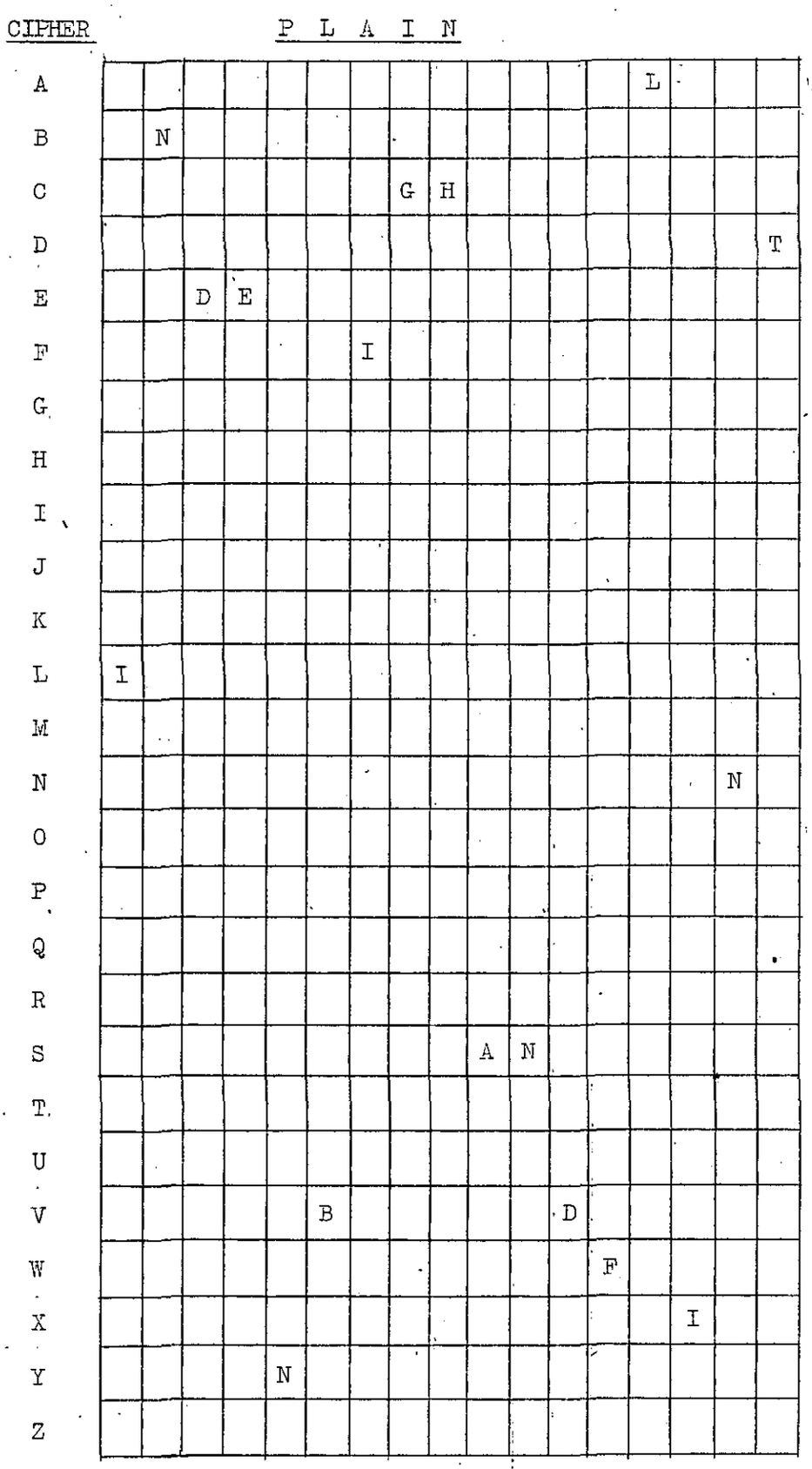
Clear Text: CARBONIFEROUS ROCKS OCCUPY PART OF THE NORTHERN COAST STOP.

4b. Let us assume that either the plain or the cipher component is the normal alphabetic sequence and that there is a progression of 1. This gives us the following two possibilities for our Vigenère table:-

I

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

II



Of these No. II is the more promising since in it, for example, three occurrences of the letter N all lie on the same diagonal, and also we find the sequences DE and GH. By completing the diagonals we obtain the following partial sequence

B A N . . . D E F G H I . L . . . . . T . . . . . .

Alphabetical considerations enable us to extend this to

B A N . . . D E F G H I $\frac{J}{K}$ L . . . . . T U V W X Y Z

This, therefore, is the plain component, and the cipher component is the normal alphabetic sequence. It is also clear that our original assumption of a progression of 1 is correct.

Translation of the cipher text enables us to complete the plain component.

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

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

Clear Text: IN DENBIGH AND FLINT THE CARBONIFEROUS LIMESTONES FORM LONG CONTINUOUS ESCARPMENTS STOP.

5. 1. Decimation Interval 9. Key phrase: BRITANNIA RULES THE WAVES.

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

2. Decimation Interval 15. Key phrase: PANZER DIVISION.

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

3. Decimation Interval 19. Key phrase: PANZER DIVISION.

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

4. Decimation Interval 17. Key phrase: WILLIAM SHAKESPEARE.

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

5. Decimation Interval 13. Key phrase: PHANTASMAGORIA.

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

6. Decimation Interval 13. Key phrase: XEROPHYTIC AZALEAS.

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

7. Decimation Interval 2. Key phrase: THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG.

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

6. The following repeats are found in the cipher text:

G H U F	Positions	94,276	Interval 182
V J R Q P	"	145,197	" 52
N Y G L	"	175,383	" 208

These are sufficient to justify an assumption that the period is 26. (It may be only 13, but it is safer to assume 26).

The text is now searched for pattern repeats, and the following are found:

(1) Z H B P G R G E I Z T W O K H W
X K Q Y F O F V P X M R S A K R (Interval 21)

(2) E P E Y T Y V J R Q P
R Z R X D X O C A H Z (Interval 25)

(3) J J P E Z E
Z Z L H T H (Interval 8)

(4) L X L B F O X
C M C N S J M (Interval 8)

If we assume a progression of 1, we shall have the relative intervals between the various letters in these pattern repeats. These intervals are shown in brackets above; e.g. In (1) X and K will be 21 places further on in the cipher component than Z and H respectively. This enables us to reconstruct the cipher component:-

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

and since U is the only letter missing, it must be placed in the vacant space. The full sequence, therefore, of the cipher component is

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

The next step is to convert the cipher text into monoliteral terms with the help of the reconstructed cipher component and our assumption that there is a progression of 1. A frequency count can then be made and used to help in the solution of this monoliteral cipher. Alternatively, a guess may be made at a probable word, and a study of the monoliteral cipher repeats suggests strongly that many of them are numbers.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MONOLITERAL CIPHER FREQUENCY COUNT

CIPHER	FREQUENCY	PLAIN
A	14	P
B	7	M
C	6	Y
D		
E		
F	13	C
G	3	B
H	4	K
I	15	D
J	23	A
K	14	L
L	42	N
M	44	T
N	8	V
O	9	W
P	47	E
Q	19	I
R		
S	26	R
T	49	O
U	13	F
V	2	J
W	25	S
X	4	G
Y	14	U
Z	16	H

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

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

(Note. - The cipher and plain component sequences are formed respectively from the first eight lines of Pinocchio and the first paragraph of Mein Kampf).

Clear Text. RECONNAISSANCE COMPLETED AT SEVENTEEN THIRTY FIVE HOURS (STOP). OLDHAMPTON HELD BY ENEMY, STRENGTH UNKNOWN (STOP). FOUR ENEMY TANKS HALTED AT SEVENTEEN OWE OWE HOURS AT ROAD JUNCTION FOUR THREE FIVE SEVEN FOUR TWO (STOP). TWO INFANTRY GUNS IN ACTION AT POINT THREE HUNDRED YARDS NORTH OF SECOND OWE IN OLDHAMPTON (STOP). RIGHT FORWARD POST OF FOURTEENTH DIV. RECONNAISSANCE BATTALION LOCATED ROAD JUNCTION THREE FIVE SEVEN FOUR (STOP). SKETCH AND COMPLETE REPORT FOLLOWS (STOP). LOCATION MOBILE GROUP STILL UNKNOWN.

SECTION V

COMPLEX SUBSTITUTION

1. In all cases one has to rely on repeats between messages in order to get sufficient depth to recognise any limitation that there may be.

(i)

Subtractor	86109	35472	45913	60872	35490	57924
Code Groups	06389	20187	04235	12158	24134	08625
Cipher	82488	55559	49148	72920	59524	55549
Code Groups	14213	16728	23964	03579	01086	12965
Cipher	90312	41190	68877	63341	36476	69889

In any column the first digits of each group of five can never vary by more than 2 even when a Subtractor is applied. If, therefore, one has a series of first digits of groups which vary from those in another text only by 1 or 2, one may assume that they are at the same part of the Subtractor.

Furthermore, if in any column the first digits were limited to, say, 3, 4 and 5, one would immediately assume that the code book was limited from 00000 to 29999 and would identify the particular digit of the Subtractor at that point as 3.

(ii)

Subtractor	8610	9354	7245	9136	0872	3549
Code Groups	3751	9735	0264	4826	4462	1531
Cipher	1361	8089	7409	3952	4234	4070
Code Groups	2024	6422	9551	1133	5713	2242
Cipher	0634	5776	6796	0269	5585	5781
	EOO	EEC	OEO	EEO	EOO	EOO

In any column the results of adding the 1st digit to the 2nd, the 2nd to the 3rd, and the 3rd to the 4th will be the same in so far as odd and even results will coincide, e.g. in column 1 above the result for every group in the column will be in the form Even, Odd, Odd. Naturally the particular form depends on the form of the subtractor at the point in question.

(iii)

Subtractor	86109	35472	45913	60872	35490	57924
Code Groups	23799	34625	42680	93738	41357	64712
Cipher	09898	69097	87593	53500	76747	11636
Code Groups	86150	27740	98760	73064	31024	86745
Cipher	62259	52112	33673	33836	66414	33669

In any column the non-carrying sum of the digits of each group will be the same, dependent upon the non-carrying sum of the subtractor at the point in question, e.g. in column 1 above the non-carrying sum of the digits of the first group in Message A is 4, and that of Message B is 4.

(iv) The limitation is of no help to the cryptanalyst.

(v)

Subtractor	86109	35472	45913	60872	35490	57924
Code Groups	15682	37118	63258	71365	47213	21087
Cipher	91781	62580	08161	31137	72603	78901
Code Groups	81346	45249	27861	93005	25561	00462
Cipher	67445	70611	62774	53877	50951	57386
	O	E	E	O	E	O/E

In any column the second digits of each group will be either all Odd or all Even, except when the code group begins with 00 (as in column 6 in the example above).

(vi)

Subtractor	8610	9354	7245	9136	0872	3549
Code Groups	0834	3298	0671	9827	6415	0573
Cipher	8444	2542	7816	8953	6287	3012
Code Groups	6123	0105	9213	3106	9228	3114
Cipher	4733	9459	6458	2232	9090	6653

In any column the first digits of each group will be limited to four particular digits:- 0, 3, 6, 9 or 1, 4, 7, 0 or 2, 5, 8, 1 etc.

2. In each group of five digits the 2nd digit will be an Even number except where a group either in the Subtractor or in the Code Book begins with 00. In the former case the majority of the second digits will be Odd, in the latter case the majority will be Even.

3.

Subtractor	78954	12341	25897	81905	89008	68978
Code Groups	26514	10259	05302	08845	05611	23851
Cipher	94468	22590	20199	89740	84619	81729
Code Groups	0....	0....	2....	1....	1....	2....
Cipher	7....	1....	4....	9....	9....	8....
Code Groups	2....	1....	1....	0....	1....	1....
Cipher	9....	2....	3....	8....	9....	7....
Code Groups	1....	2....	1....	2....	2....	0....
Cipher	8....	3....	3....	0....	0....	6....

Presumably it will be very rare that any first digit of a code group will be higher than 2, so that if in any column there are 3 different first digits, the digit of the subtractor at that point can be established. e.g. in the example above the first digits of every group of five in the subtractor can be more or less certainly established, as can also, of course, the first digits of the basic code groups.

It is quite probable that the beginnings of messages will be of a stereotyped form, so that if in the example above we assume that the 1st message starts TO GENERAL COMMANDING, we may make a good guess at the probable second digit of the basic code group and, therefore, of the digit of the Subtractor at the same point. If our assumptions are correct, we shall have the following partial Subtractor

78 | .. | .1 | 2. | .. | 25 | .. | ....

which, on reference to the substitution table, becomes

N	.	D	A	.	A
T	.	E	B	.	
W	.	.	O	.	

We might now assume that the first word of the Subtractor is THE (789541), which will, if correct, give us basic groups throughout the first column. For example, we shall now know that TO is 26514.

Thereafter solution may be achieved by anagramming the Subtractor against the messages and guessing at probable words in both. Naturally the process of guessing words in the messages becomes progressively easier as the places of more words in the original dictionary are found. It is to be noted that where the word in the message begins with the letter A, the chances are that the first two digits of the basic group will be 00 and, therefore, in the final enciphered form the first two digits will be those of the Subtractor at that point.

4. Anagramming of the Subtractor would become much more difficult. It is to be noted that there would be a large proportion of '4's in the Subtractor owing to the high frequency of the letters E and O.

5. From columns B and D it is clear that the second term of the message is 24351. Hence to reduce the second term of message 2 (22775) to this we must have for column C a Provisional Subtractor of 08424.

It is now clear from columns B and C that the first term of the message is 14820. Hence for column A the Provisional Subtractor will be 27072.

Similarly from columns C and D it is clear that the third term of the message is 14577. Hence for column E the Provisional Subtractor will be 05306.

	A	B	C	D	E	F	G
	27072	40186	08424	71003	05306	47419	66328
1.	14820	24351	14577	11381	40000	40473	35127
2.		14820	24351	14577	11381	40000	42284
3.			14820	24351	14577	11381	40000
4.	40000	40473	35127	02771	36064	09320	12030
5.	28420	17143	28420	14629	58404	42284	40473
6.	17848	40000	42284	16914	17143	35127	58404
7.	42284	14272	36524	42284	37935	42255	45262
8.	06729	01536	41528	36236	32048	40000	48530
9.	20238	06729	13823	36524	29959	04905	35127
10.	29959	04905	35127	40000	42284	40473	35127
11.	07395	36064	04222	43869	07035	04905	35127
12.	36693	40000	44245	40000	42404	40000	14015
13.	27810	20277	23624	09320	17484	17848	08166
14.	58088	58323	09320	59009	13255	08329	40000
15.	48530	18820	35127	36689	42255	06414	36524

6. Let A be the basic column, then the terms 54906 in column B and 12244 in column C have to be reduced to 31892. When this has been done, it will be clear that the terms 85570 in column D and 19873 in column E have to be reduced to the 31549, which has now been produced in columns B and C. Finally the terms 87419 in column F and 06328 in column G are reduced to the 67072 which has been produced in column E.

	A	B	C	D	E	F	G
	00000	23114	81452	54031	88334	20447	49356
1.	31892	64437	12991	82384	45306	87882	91445
	31892	*41323*	*31549*	*38353*	*67072*	*67445*	*52199*
2.		54906	22775	85570	16687	87419	08502
		31892	*41323*	*31549*	*38353*	*67072*	*69256*
3.			12244	95354	19873	58790	06328
			31892	*41323*	*31549*	*38353*	*67072*

7. If there are 3 groups x, y, z in common in a pair of columns, then Differences will appear in the columns as

x - y (or y - x)
x - z (or z - x)
y - z (or z - y)

i.e. there will be 3 differences appearing the same in the two Difference Tables, and their positions in the table will be at the corners of a right-angled triangle.

8.

01536	1	11381	3	20238	1	32048	1	40000	11	58088	1
02771	1	12030	1	20277	1	35127	8	40473	4	58323	1
04222	1	13255	1	23624	1	36064	2	41528	1	58404	2
04905	3	13823	1	24351	3	36236	1	42255	2	59009	1
06414	1	14015	1	27810	1	36524	3	42284	6		
06729	2	14272	1	28420	2	36689	1	42404	1		
07035	1	14577	3	29959	2	36693	1	43869	1		
07395	1	14629	1			37935	1	44245	1		
08166	1	14820	3					45262	1		
08329	1	16914	1					48530	2		
09320	3	17143	2								
		17484	1								
		17848	2								
		18820	1								

DIFFERENCE TABLE

	42284	40473	35127	04905	36524
40000	02284	00473	15983	46105	14586
42284		02811	17167	48389	16760
40473			15356	46578	14959
35127				31222	09603
04905					32629
36524					

9.

From Column A 70022 - 78848 = 02284
" Difference Table of Ex. 6. 42284 - 40000 = 02284

∴ Subtractor is 38848

From Column B 23766 - 23393 = 00473
" Difference Table of Ex. 8. 40473 - 40000 = 00473

∴ Subtractor is 83393

From Column C 68334 - 53088 = 15356
" Difference Table of Ex. 8. 40473 - 35127 = 15356

∴ Subtractor is 28961

From Column D 71256 - 64199 = 17167
" Difference Table of Ex. 8. 42284 - 35127 = 17167

∴ Subtractor is 39072

From Column E 32419 - 27163 = 15356
" Difference Table of Ex. 8. 40473 - 35127 = 15356

∴ Subtractor is 92046

From Column F 89775 - 87591 = 02284
" Difference Table of Ex. 8. 42284 - 40000 = 02284

∴ Subtractor is 47591

	A	B	C	D	E	F
	38848	83393	28961	39072	92046	47591
16.	40000	40473	35127	58323	36064	09320
17.	36236	32048	36064	42284	40473	35127
18.	42284	16914	58323	17143	58404	42284
19.	42284	41735	26236	32048	35127	40000
20.	42404	40000	14015	58404	13213	40000
21.	36693	40000	44245	07395	42404	40000
22.	35127	26521	07152	09498	20939	17848
23.	43869	42284	40473	35127	40000	07026

This is checked by the numerous offset recurrences.

GROUPS ALREADY OCCURRING IN TABLE OF EXERCISE 8											
07395	1	14015	1			32048	2	40000	7	58323	2
09320	1	16914	1			35127	5	40473	3	58404	2
		17143	1			36064	2	42284	5		
		17848	1			36236	1	42404	2		
						36693	1	43869	1		
								44245	1		
GROUPS NOT OCCURRING IN TABLE OF EXERCISE 8											
07026	1	13213	1	20939	1			41735	1		
07152	1			26236	1						
09498	1			26521	1						

10. (a) METHOD OF DISCOVERING WHETHER TWO PROVISIONAL SUBTRACTORS ARE INTER-RELATED BY 'NON-COINCIDENCE OF CUT'.

Suppose that there are two texts A and B with different Provisional Subtractors and that the particular Provisional Subtractor in the case of text A has equated all the columns to column one. Now a Provisional Subtractor must be found for text B, which will equate all of its columns to column one of text A.

If it is suspected that B subtractor is a 'cut' of A subtractor, cut A subtractor and compare the inter-column intervals thus formed with those of B subtractor (or vice versa). If the intervals, treated as cyclic, are the same, the two subtractors are inter-related by 'non-coincidence of cut'.

e.g. In Section I, Exercise 14, Provisional Subtractors are found equating both sets of text to the first column of Text 1.

A. 00 13 47 79 61 44 83 96 03 77 26 45 34

B. 66 57 88 55 90 82 71 68 29 52 95 14 32

A is 'cut' and it is found that the pairs thus formed produce intervals which correspond with those of B.

A 'cut': 01 34 77 96 14 48 39 60 37 72 64 53 40

B : 29 52 95 14 32 66 57 88 55 90 82 71 68

(b) METHOD OF USING 'NON-COINCIDENCE OF CUT' IN ORDER TO ARRIVE AT THE TRUE FIGURES OF A COMPLEX SUBSTITUTION CIPHER.

In order to arrive at a Basic Subtractor a number must be found such that when it is added to the columns of the Provisional Subtractors A and B, it will produce the same result - in one case, however, the result will be on the 'cut'.

e.g. The following two subtractors are A 'cut' and B fitted together as explained above and with the original columns marked:

A 'cut': 0|1 3|4 7|7 9|6 1|4 4|8 3|9 6|0 3|7 7|2 6|4 5|3 4|0

B : |2 9|5 2|9 5|1 4|3 2|6 6|5 7|8 8|5 5|9 0|8 2|7 1|6 8|

Consider the beginning terms:

x_1 x_2 y_1 y_2

A 'cut': 0|1 3|4 7|

B : 2 9|5 2|9 5|

p_1 p_2 q_1 q_2

Whatever is added to x_1, must also be added to p_1, and whatever is added to x_2 must also be added to p_2, and so on. The object is to make x_2 the same as p_1, y_1 the same as p_2, etc.

If 0 is added to x_1 (1), it must also be added to p_1 (5) $\therefore$ p_1 will equal 5. Clearly since x_2 has got to be the same as p_1, 2 will have to be added to it.

Similarly, if 0 is added to y_1, it must also be added to q_1. The result in the latter case is 9. Clearly 2 must be added to y_2 in order to obtain the same result.

Thus 02 is one result, but obviously there are 10 possible solutions:- 02, 13, 24, 35, 46, 57, 68, 79, 80, 91.

i.e. 10 different subtractors are possible:-

(i)	21	54	97	16	34	68	59	80	57	92	84	73	60
(ii)	32	65	08	27	45	79	60	91	68	03	95	84	71
(iii)	43	76	19	38	56	80	71	02	79	14	06	95	82
(iv)	54	87	20	49	67	91	82	13	80	25	17	06	93
(v)	65	98	31	50	78	02	93	24	91	36	28	17	04
(vi)	76	09	42	61	89	13	04	35	02	47	39	28	15
(vii)	87	10	53	72	90	24	15	46	13	58	40	39	26
(viii)	98	21	64	83	01	35	26	57	24	69	51	40	37
(ix)	09	32	75	94	12	46	37	68	35	70	62	51	48
(x)	10	43	86	05	23	57	48	79	46	81	73	62	59

11.

(i) By the method of the previous Exercise

Message 1 reduced to the common Base of Column A (see Exercise 6) is

31892 41323 31549 38353 67072

and the Provisional Subtractor is

00000 23114 81452 54031 88334

To equate Message 24 to the same as Message 1 above, we must have the following Provisional Subtractor

14223 45369 28746 54539 97563

These two Provisional Subtractors are set against each other

x_1	x_2															
0	0	0	0	0	2	3	1	1	4	8	1	4	5	2	.....	
	1	4	2	2	3	4	5	3	6	9	2	8	7	4	6	.....
p_1	p_2															

What must be added to the columns of each to produce the same result?

If 0 is added to x_1, it must also be added to p_1. In the latter case the result is 1. Now this result must also be obtained by adding something to x_2. Clearly 1 has to be added. Thus the first two figures of the Basic Subtractor are 01, and continuing the process we have 01579.

When this is added to the Provisional Subtractor for Message 1, it produces

01579 24683 82921 55500 89803

As has been seen in Exercise 10, there are nine other possible solutions, but since it is known that the Subtractor starts with 2 (see para. 11), we shall select

23791 46805 04143 77722 01025

(ii) By another method

Assuming that Message 24 starts with the same clear Text as Message 1, we set the two messages against each other

31892 64437 12991 82384 45306 87882

4501 58668 25928 58288 25453 5

The digit 3 of column 1 has become 4 in column 2. Hence, if the first digit of the Subtractor is 0, the second must be 1. Similarly the digit 1 of column 2 has become 5 in column 3. Hence, if the second digit of the Subtractor is 1, the third must be 5. Continuing the process we have

01579 24683 82921 55500 89803 2

But since we know that the first term of the Subtractor is actually 2, we shall add this digit throughout and produce

23791 46805 04143 77722 01025 4

By considering the beginning groups of Messages 1, 2 and 3, we may continue this method and produce

(01025) 43138 62047.

To obtain the true figures of the Basic Book 04381 must be added to each of the groups in the Tables of Exercises 8 and 9.

This means that for Message 16 (Exercise 9) the true groups are

44381 44754 39408 52604 30345 03601

Since they actually appear as

78848 23766 53088 87395 28000 46811

it is clear that the Basic Subtractor at this point is

34567 89012 24680 35791 98765 43210

R. From a preliminary inspection it appears that since the first group of every message consists of consecutive digits (or 00000), this group is non-textual.

The messages, except for those beginning with the group 00000, may be set in depth by means of the check groups which occur every eleventh group. It is found that, excluding check groups, there are 100 groups in the Subtractor.

Owing to the occasional impossibility of fitting in the beginning and end of messages with the check groups, it becomes clear that there are 2 Indicator Groups in every message. When repeats are lined up it becomes clear that the particular groups in question are the third from the beginning and the third from the end (excluding the non-textual first group).

THE INDICATOR SYSTEM

The Indicator is a 5-figure group in which the first 3 digits are the total number of digits in the message proper (i.e. excluding check groups), and the last 2 digits indicate the starting (or finishing) point on the Subtractor. The Indicator with the starting point is then added to the second group of the message proper and inserted after that group; the Indicator with the finishing point is added to the penultimate group of the message and inserted before that group.

e.g. Messages 1 and 2 start in the same column and end in adjacent columns.

Message 1		Message 2	
Concealed Indicator (3rd Group)	85760	Concealed Indicator (3rd Group)	84260
2nd Group	74769	2nd Group	74769
Actual Indicator	110,01	Actual Indicator	105,01
Concealed Indicator (Antepenultimate Group)	19298	Concealed Indicator (Antepenultimate Group)	79319
Penultimate Group	08276	Penultimate Group	69898
Actual Indicator	110,22	Actual Indicator	105,21

METHOD OF OBTAINING A PROVISIONAL BASE

The following portions of messages have been set in depth with the aid of the check groups:-

	A	B	C	D	E	F	G	H	J
1.	[60730	74769	97799	11228	73928	65464	05744	50524	78007...
2.	[60730	74769	03391	18187	52608	65464	17243	64171	07778...
3.	...73077	56769	67046	94811	51690	43998	23359	04198	80160...
5.				[85486	47842	65464	70505	29830	87014...
8.	[83185	93757	87550	31934	14969	29692	23363	60274	81885...
12.	...47135	70400	87569	84180	00854	12944	18406	34459	79225...
13.	...05042	22899	08618	97104	09620	49527	95207	50656	08547...
16.	...91669	69083	79291	73568	28854	75700	22645	90584	64880]
17.							[06788	67332	20013...
22.	[60730	74769	03391	18187	52608	65464	71543	87203	79225...
24.	...70210	08694	52962	96934	67027	70558	16312	49097	12685...
25.	[83185	93757	87550	50241	67713	14676	96743	83197	33083...
27.	...95948	73602	53544	13945	73843	65202	18406	72170	97750...
29.			[52487	63198	78601	86447	18244	72350	47851...

Since Messages 2 and 29 are both to Station X it may be assumed that in actual fact they start with the same groups, and since Messages 2 and 22 which are both to X show a repeat of 6 groups it may be assumed that this is probably the length of the stereotyped beginning. Similarly Messages 5, 8 and 17 are all to C.Q. and the repeat between Messages 8 and 25 show that in this case the stereotyped beginning extends over only three groups. This information is sufficient to enable us to equate all of the columns B to J to Column A.

	A	B	C	D	E	F	G	H	J
	00000	13972	92757	02301	67067	70661	23603	87557	35210
1.	[60730	61897	05042	19927	16961	95803	82141	73077	43897...
2.	[60730	61897	11644	16886	95641	95803	94640	87624	72568...
3.	...73077	43897	75399	92510	94633	73337	00756	27641	55950...
5.				[83185	80885	95803	57902	42383	52804...
8.	[83185	80885	95803	39633	57902	59031	00760	83727	56675...
12.	...47135	67538	95812	82889	43897	42383	95803	57902	44015...
13.	...05042	19927	16961	95803	42663	79966	72604	73109	73337...
16.	...91669	56111	87544	71267	61897	05149	09042	13037	39670]
17.							[83185	80885	95803...
22.	[60730	61897	11644	16886	95641	95803	58940	00756	44015...
24.	...70210	95722	60215	94633	00060	00997	93719	62540	87475...
25.	[83185	80885	95803	58940	00756	44015	73140	06640	08873...
27.	...95948	60730	61897	11644	16886	95641	95803	95623	62540...
29.			[60730	61897	11644	16886	95641	95803	12641...

This now gives us the Provisional Basic groups for the addresses of Messages to Y, such as Message 1, and for the endings of Messages from Q, such as Message 16.

It will be found that by this method Provisional Subtractors can be found for all but twenty-two of the hundred columns. To obtain Subtractors for these twenty-two remaining columns Difference Tables may be constructed for them and then compared with a Difference Table compiled from commonly-occurring terms in the Provisional Base. An alternative method would be to get out as much of the clear text as possible from the columns already reduced to a provisional base, and use the clear text itself to establish missing columns.

METHOD OF BREAKING INTO THE BOOK

The following is a list of the addresses in the Provisional Base:

To X. (Gallina) 60730 61897 11644 16886 95641 95803

To Y. (Antonelli) 60730 61897 05042 19927 16961 95803

To Q. (Argentino) 60730 61897 05149 09042 13037 95803

To S. (Berginzoli) 60730 61897 06760 11886 30064 95623 95803

It may be assumed that the frequently-occurring group 95803 represents STOP. From the message in clear which is given, it seems reasonable to suppose that 60730 = FOR and 61897 = GENERAL. This means that the remaining groups must represent the generals' names. The following scheme seems to fit very reasonably from the numerical order of the groups even with our Provisional Base:-

To X. 60730 61897 11644 16886 95641 95803.

FOR GENERAL GAL LIN A STOP

To Y. 60730 61897 05042 19927 16961 95803.

FOR GENERAL ANT ONE LLI STOP

To Q. 60730 61897 05149 09042 13037 95803.

FOR GENERAL ARG ENT INO STOP

To S. 60730 61897 06760 11886 30064 95623 95803

FOR GENERAL BER GIN ZOL I STOP

GROUPS IN NUMERICAL ORDER

05042 ANT	60730 FOR	95623 I
05149 ARG	61897 GENERAL	95641 A
06760 BER		95803 ⊙
09042 ENT		
11644 GAL		
11886 GIN		
13037 INO		
16886 LIN		
16961 LLI		
19927 ONE		
30064 ZOL		

In the columns obtained in a provisional base it will be noticed that half way through the last but one message are the groups FOR GENERAL GALLINA STOP I, and also the message ends GENERAL BERGINZOLI (and 3 groups). Now we know that in actual fact the message is sent to all stations by General Gallina and not by General Berginzoli. Furthermore it is the only message of that type which is not sent out at midday. Could it be in part an encipherment of the previous message which is in clear? The latter starts FOR GENERAL GALLINA. I..... and ends GENERAL BERGINZOLI. Also the message with which we are concerned was sent out by the recipient of the clear text message and its time of interception is only 20 minutes later. Indeed, everything points to our assumption being correct. If so, we may assign values to the groups as follows:-

60730	61897	11644	16886	95641	95803	95623	62540
FOR	GENERAL	GAL	LIN	A	STOP	I	HAVE
61198	73337	95722	87475	48961	80005	95803	61897
GIVEN	ORDER	S	TO	CEASE	RESISTANCE	STOP	GENERAL
06760	11886	30064	95623	39640			
BER	GIN	ZOL	I	18			

Consider the group 39640 which represents the number 18. It seems reasonable to suppose that in the true Base the group ends 018. If this is so, it enables us to correct the last three digits of every group so that they stand in true Base form, i.e. 632 must be subtracted from the last 3 digits of all groups. When this has been done to the groups which we have fixed as representing single letters of the alphabet, we have the following values:

95019 = **A** ; 95091 = I ; 95190 = **S**.

This leads immediately to assumption of groups for the whole single - letter alphabet as follows:

95019 A	95082 H	95154 O	95208 U
95028 B	95091 I	95163 P	95217 V
95037 C	95109 J	95172 Q	95226 W
95046 D	95118 K	95181 R	95235 X
95055 E	95127 L	95190 S	95244 Y
95064 F	95136 M	95199 T	95253 Z
95073 G	95145 N		

[N.B. Later it will be found that in actual fact the group 95199 is omitted, so that 95208 is T, 95217 is U, etc.].

Consider now the groups which represent trigraphs. When their last three digits are reduced to the true base, we have the following values:

05410	ANT	11012	GAL	16339	LLI
05517	ARG	11254	GIN	19395	ONE
06138	BER	13405	INO	30432	ZOL
09410	ENT	16254	LIN		

When it is realised that, considering the last letter of each trigraph, T is the 20th letter of the alphabet, G the 7th, R the 18th, L the 12th, and so on, the last 2 digits of each group at once become significant.

If 05410 = ANT, then probably 05390 = ANA
and if 05517 = ARG, " " 05510 = ARA

Hence we may assume that the sequence runs

05390	ANA
05420	AOA
05450	APA
05480	AQA
05510	ARA

Furthermore, when we consider the first 2 digits of each group, we notice that trigraphs with A start 05, with B start 06, with E (three letters further on in the alphabet) start 09, and so on.

Hence we may construct a table for Trigraphs as follows:

	1st LETTER +	2nd LETTER +	3rd LETTER
A	05000	000	01
B	06000	030	02
C	07000	060	03
D	08000	090	04
E	09000	120	05
F	10000	150	06
G	11000	180	07
H	12000	210	08
I	13000	240	09
J	14000	270	10
K	15000	300	11
L	16000	330	12
M	17000	360	13
N	18000	390	14
O	19000	420	15
P	20000	450	16
Q	21000	480	17
R	22000	510	18
S	23000	540	19
T	24000	570	20
U	25000	600	21
V	26000	630	22
W	27000	660	23
X	28000	690	24
Y	29000	720	25
Z	30000	750	26

When the values thus obtained have been inserted throughout the cipher texts, it will furnish sufficient evidence for finding the values of the other groups. It will be found that there is also a table of Digraphs. Further, in order to get all groups of the Vocabulary in numerical and alphabetical order, a correction will have to be made to the first digit of every group, by subtracting 4.

Thus the further Subtractor needed to reduce to true Base all the groups of our provisional base is 40632.

The full Code Book is found to be as follows:-

CODE BOOK

TABLE I. SINGLE LETTERS AND PUNCTUATION

A 55019	H 55082	O 55154	U 55217
B 55028	I 55091	P 55163	V 55226
C 55037	J 55109	Q 55172	W 55235
D 55046	K 55118	R 55181	X 55244
E 55055	L 55127	S 55190	Y 55253
F 55064	M 55136	T 55208	Z 55262
G 55073	N 55145		

. 55271	(55299	" 55316
, 55280	) 55307	" 55325

TABLE II. DIGRAPHS

	1st LETTER + 2nd LETTER			1st LETTER + 2nd LETTER	
A	60000	01	N	60390	14
B	60030	02	O	60420	15
C	60060	03	P	60450	16
D	60090	04	Q	60480	17
E	60120	05	R	60510	18
F	60150	06	S	60540	19
G	60180	07	T	60570	20
H	60210	08	U	60600	21
I	60240	09	V	60630	22
J	60270	10	W	60660	23
K	60300	11	X	60690	24
L	60330	12	Y	60720	25
M	60360	13	Z	60750	26

TABLE III. TRIGRAPHS

	1st LETTER	+ 2nd LETTER	+ 3rd LETTER
A	65000	000	01
B	66000	030	02
C	67000	060	03
D	68000	090	04
E	69000	120	05
F	70000	150	06
G	71000	180	07
H	72000	210	08
I	73000	240	09
J	74000	270	10
K	75000	300	11
L	76000	330	12
M	77000	360	13
N	78000	390	14
O	79000	420	15
P	80000	450	16
Q	81000	480	17
R	82000	510	18
S	83000	540	19
T	84000	570	20
U	85000	600	21
V	86000	630	22
W	87000	660	23
X	88000	690	24
Y	89000	720	25
Z	90000	750	26

TABLE IV. NUMERALS

99000 + Numeral required.

TABLE V. VOCABULARY

00108	About	07783	Cannot	20032	Folk
01823	Accident	07856	Cap	20040	Following
02031	Acknowledge	07918	Captain	20058	Food
02124	Acute	07940	Car	20108	For
02464	Aerodrome	08074	Carry	20128	Force
02579	After	08208	Casualty	20365	Forward
02751	Air	08339	Cease	20431	Fourth
02870	All	08724	Check	20683	From
02968	Almost	09066	Cipher	20922	Further
02986	Already	09896	Colonel	21143	Garrison
02988	Also	10033	Command	21265	General
03265	And	10188	Communication	21512	Give
03485	Anti	11342	Continue	21516	Given
03727	Appoint	11344	Continuous	22289	Ground
04071	Arrive	12272	Craft	22308	Group
04127	Artillery	12433	Crew	22658	Hand
04137	As	13068	Damage	22918	Have
04423	At	13222	Dawn	22968	He
04483	Attack	13601	Defence	23089	Heavy
05263	Base	14060	Depot	23237	Here
05341	Battalion	14304	Destroy	23336	High
05513	Become	14306	Destroyed	23512	Hold
05562	Been	15328	Dispatch	23790	Hour
05575	Before	15687	Dive	24308	Imagine
05603	Begin	15812	Document	24596	Impossible
05635	Being	16043	Down	24724	In
05686	Belong	16589	Early	25213	Indecipherable
06482	Bomb	17370	Enemy	25632	Infantry
06488	Bombardment	18084	Exceptional	26324	Intense
06493	Bomber	18318	Expect	26475	Intermittent
07016	Bring	18940	Far	27031	Its
07055	British	19401	Fifth	27093	January
07409	But	19409	Fight	27418	Just
07503	By	19525	Fire	27571	Kill

27906	Land	33933	Outer	43195	Shot
27942	Language	34086	Over	43365	Sign
28029	Last	34401	Owing	43455	Since
28101	Launch	34725	Parachute	43553	Situation
28328	Left	34932	Party	43782	Slight
28594	Lieutenant	35361	Penetrate	44088	So
28596	Lieutenant-Colonel	35767	Petrol	44262	Soon
29045	Long	36190	Plain	44376	South
29047	Longer	36310	Please	45339	Still
29490	Made	36768	Possible	46295	Support
29616	Major	37519	Prisoner	46807	Taken
29754	Man	38661	Quick	46914	Tank
30688	Message	38725	Quite	47092	Telegram
30780	Midday	38861	Raid	47358	That
31635	Morning	39001	Rank	47367	The
31719	Motor	39183	Reach	47384	Them
31888	Much	39334	Receipt	47430	These
32021	Must	39391	Receive	47491	This
32072	My	39559	Red	47843	To
32558	Night	39619	Reduce	47912	Tomorrow
32591	Ninth	39677	Refer	48344	Transmit
32619	No	39816	Regiment	48883	Tuesday
32790	Not	40212	Repeat	49647	Under
32936	Number	40238	Replace	50294	Unlikely
33351	Of	40253	Report	51037	Until
33355	Off	40473	Resistance	51835	Very
33390	Offer	40608	Result	52867	Were
33411	Officer	41440	Run	52869	West
33445	Oil	41590	Safely	52954	When
33518	On	42257	Sea	52988	Which
33558	Open	42389	Secret	53187	Will
33577	Operation	42519	Send	53637	Wound
33705	Order	42562	Sent	53946	Yesterday
33855	Other	42826	Severe	53959	Yet
33874	Our	43036	Shell	54001	You
33889	Out	43173	Short	54018	Your

TABLE VI. THE SUBTRACTOR

00	01	02	03	04	05	06	07	08	09	CHECK
02975	40632	53504	32389	42933	07699	10293	63235	27189	75842	09597
10	11	12	13	14	15	16	17	18	19	CHECK
59692	85542	08333	71062	94069	66616	45647	26593	29737	62727	75938
20	21	22	23	24	25	26	27	28	29	CHECK
93569	53267	90102	82520	23159	57305	86418	10514	10916	03587	36730
30	31	32	33	34	35	36	37	38	39	CHECK
72040	58555	95244	24025	02186	24485	75233	01662	86703	38507	08884
40	41	42	43	44	45	46	47	48	49	CHECK
89816	35231	06762	06881	90847	54307	75411	67043	94550	55391	47831
50	51	52	53	54	55	56	57	58	59	CHECK
85286	18406	18101	20489	37035	08612	37322	71286	50146	70033	56788
60	61	62	63	64	65	66	67	68	69	CHECK
18384	76522	98633	79941	01500	94683	28639	73053	84153	89551	08346
70	71	72	73	74	75	76	77	78	79	CHECK
07570	65492	38731	84275	07395	97999	18260	87448	02642	57524	72296
80	81	82	83	84	85	86	87	88	89	CHECK
50135	69922	65319	56820	71217	02865	01468	01447	79902	04069	78968
90	91	92	93	94	95	96	97	98	99	CHECK
45923	86480	95907	55923	87308	31649	12885	21576	27772	57310	56912

TABLE VII. BASIC GROUPS AND PLAIN TEXT

Message 1. (Starting in Column 01)

20108	For	14060	depot
21265	General	07503	by
65410	Ant	48883	Tuesday
79395	one	19401	fifth
76339	lli	27093	January
55271	.	55271	.
42519	Send	21265	General
33445	oil	71012	Gal
03265	and	76254	lin
35767	petrol	55019	a
47843	to	99236	236

Message 2. (Starting in Column 01)

20108	For	55271	.
21265	General	08724	Check
71012	Gal	03265	and
76254	lin	40212	repeat
55019	a	55271	.
55271	.	21265	General
54018	Your	65410	Ant
47092	telegram	79395	one
32936	number	76339	lli
99236	236	99172	172
25213	indecipherable		

Message 3 (Starting in Column 95)

20108	For
21265	General
71012	Gal
76254	lin
55019	a
55271	.
33445	Oil
03265	and
35767	petrol
52988	which
54001	you
33705	order
60124	ed
87019	was
15328	dispatch
60124	ed
53946	yesterday
31635	morning
55271	.
21265	General
65410	Ant
79395	one
76339	lli
99173	173

Message 5 (Starting in Column 04)

43553	Situation
40253	report
55271	.
17370	Enemy
02751	air
12272	craft
22918	have
29490	made
99003	3
15687	dive
06482	bomb
73397	ing
04483	attack
55190	s
33518	on
33933	outer
13601	defence
55190	s
33351	of
66018	Bar
68241	dia
55271	.
13068	Damage
43782	slight
55271	.
08208	Casualty
55190	s
33411	officer
55190	s
27571	kill
60124	ed
99001	1
55280	,
53637	wound
60124	ed
99002	2
55280	,
33855	other
39001	rank
55190	s
27571	kill
60124	ed
99006	6
55280	,
53637	wound
60124	ed
99018	18
55271	.
99001	1
17370	enemy
06493	bomber
50294	unlikely
47843	to
39183	reach
27031	its
05263	base
41590	safely
55271	.
84422	Tob
82611	ruk
49647	under
26475	intermittent
06488	bombardment
20683	from
42257	sea
55271	.
21265	General
71012	Gal
76254	lin
55019	a
99237	237

Message 6 (Starting in Column 10)

20108	For
21265	General
65410	Ant
79395	one
76339	lli
55271	.
02031	Acknowledge
39334	receipt
32072	my
33577	operation
33705	order
99012	12
15328	dispatch
60124	ed
53946	yesterday
07503	by
22658	hand
33351	of
28594	Lieutenant
65410	Ant
79361	oma
82068	rch
55091	i
55271	.
21265	General
71012	Gal
76254	lin
55019	a
99238	238

Message 8 (Starting in Column 01).

43553	Situation
40253	report
55271	.
99001	1
17370	enemy
19409	fight
60138	er
43195	shot
16043	down
07503	by
03485	anti
02751	air
12272	craft
24724	in
42257	sea
33355	off
84422	Tob
82611	ruk
47491	this
31635	morning
55271	.
15687	Dive
06482	bomb
73397	ing
04483	attack
55190	s
34086	over
66018	Bar
68241	dia
02968	almost
11344	continuous
55271	.
08208	Casualty
55190	s
33411	officer
55190	s
27571	kill
60124	ed
99002	2
55280	,
53637	wound
60124	ed
99005	5
55280	,
33855	other
39001	rank
55190	s
27571	kill
60124	ed
99024	24
55280	,
53637	wound
60124	ed
99091	91
55271	.
28029	Last
32558	night
07055	British
38861	raid
73397	ing
34932	party
28328	left
99001	1
53637	wound
60124	ed
29754	man
24724	in
33874	our
22658	hand
55190	s
04423	at
66018	Bar
68241	dia
55271	.
22968	He
05686	belong
55190	s
47843	to
32591	ninth
78438	Nor
20032	folk
25632	infantry
39816	regiment
55271	.
20058	Food
43553	situation
24724	in
66018	Bar
68241	dia
05513	become
73397	ing
02124	acute
55271	.
21265	General
71012	Gal
76254	lin
55019	a
99239	239

Message 9 (Starting in Column 70)

20108	For
21265	General
71012	Gal
76254	lin
55019	a
55271	.
54018	Your
33577	operation
33705	order
32936	number
99011	11
39391	receive
60124	ed
55271	.
21265	General
65410	Ant
79395	one
76339	lli
99174	174

Message 12 (Starting in Column 90)

43553	Situation
40253	report
55271	.
17370	Enemy
06488	bombardment
33351	of
66018	Bar
68241	dia
11342	continue
55190	s
55280	,
07503	by
27906	land
55280	,
42257	sea
03265	and
02751	air
55271	.
17370	Enemy
04483	attack
24724	in
20128	force
18318	expect
60124	ed
43173	short
60355	ly
20683	from
44376	south
52869	west
03265	and
52869	west
55271	.
21265	General
71012	Gal
76254	lin
55019	a
99240	240

Message 13 (Starting in Column 99)

20108	For
21265	General
65410	Ant
79395	one
76339	lli
55271	.
02031	Acknowledge
39334	receipt
32072	my
33577	operation
33705	order
32936	number
99012	12
55271	.
21265	General
71012	Gal
76254	lin
55019	a
99241	241

Message 14 (Starting in Column 19)

20108	For
21265	General
65517	Arg
69410	ent
73405	ino
55271	.
29616	Major
65410	Ant
79399	oni
55154	o
77438	Mor
69342	ell
55091	i
55280	,
29616	Major
71241	Gia
67433	com
55154	o
67519	Cri
83459	spi
03265	and
07918	Captain
71002	Gab
82245	rie
76335	lle
55046	d
65404	Ann
85416	unz
60255	io
22918	have
04071	arrive
60124	ed
04423	at
84422	Tob
82611	ruk
55271	.
47430	These
99003	3
33411	officer
55190	s
22918	have
05562	been
03727	appoint
60124	ed
47843	to
40238	replace
47367	the
99003	3
05341	battalion
10033	command
60138	er
55190	s
53637	wound
60124	ed
24724	in
17370	enemy
02751	air
38861	raid
33518	on
68138	Der
60391	na
55271	.
36310	Please
42519	send
07940	car
20108	for

47384	them
04137	as
44262	soon
04137	as
36768	possible
55271	.
21265	General
71012	Gal
76254	lin
55019	a
99242	242

Message 15 (Starting in Column 30).

21265	General
71012	Gal
76254	lin
55019	a
55271	.
33705	Order
55190	s
22918	have
05562	been
21512	give
55145	n
00108	about
15328	dispatch
33351	of
07940	car
47843	to
39183	reach
72434	Hon
05575	before
30780	midday
47912	tomorrow
47843	to
07016	bring
23237	here
99003	3
33411	officer
55190	s
39677	refer
39559	red
47843	to
24724	in
54018	your
47092	telegram
32936	number
99242	242
55271	.
21265	General
65517	Arg
69410	ent
73405	ino
99047	47

Message 16 (Starting in Column 80).

21265	General
71012	Gal
76254	lin
55019	a
55271	.
34401	Owing
47843	to
01823	accident
07940	car
39677	refer
39559	red
47843	to
24724	in
32072	my
32936	number
99047	47
33351	of
53946	yesterday
07783	cannot
39183	reach
72434	Hon
51037	until
16589	early
47912	tomorrow
31635	morning
21265	General
65517	Arg
69410	ent
73405	ino
99048	48

Message 17 (Starting in Column 07).

43553	Situation
40253	report
55271	.
43036	Shell
73397	ing
45339	still
51835	very
23089	heavy
04423	at
66018	Bar
68241	dia
55280	,
07409	but
32619	no
43365	sign
53959	yet
33351	of
18318	expect
60124	ed
17370	enemy
04483	attack
55271	.
16589	Early
47491	this
31635	morning
17370	enemy
02751	air
12272	craft
08074	carry
60124	ed
33889	out
23089	heavy
06482	bomb
73397	ing
04483	attack
33518	on
02464	aerodrome
04423	at

66134	Ben
73391	ina
55271	.
99002	2
07856	Cap
82434	ron
55091	i
06493	bomber
55190	s
52867	were
14304	destroy
60124	ed
33518	on
22289	ground
55271	.
99001	1
17370	enemy
87132	Wel
76254	lin
71585	gto
55145	n
06493	bomber
87019	was
43195	shot
16043	down
07503	by
03485	anti
02751	air
12272	craft
55271	.
99003	3
33351	of
12433	crew
27906	land
60124	ed
07503	by
34725	parachute
03265	and
52867	were
46807	taken
37519	prisoner
55271	.
21265	General
71012	Gal
76254	lin
55019	a
99243	243

Message 19 (Starting in Column 50).

21265	General
71012	Gal
76254	lin
55019	a
55271	.
09896	Colonel
71255	Gio
86014	van
60399	ni
82606	Ruf
60165	fo
87019	was
27571	kill
60124	ed
53946	yesterday
24724	in
31719	motor
01823	accident
55271	.
21265	General
65517	Arg
69410	ent
73405	ino
99049	49

Message 20 (Starting in Column 20).

20108	For
21265	General
71012	Gal
76254	lin
55019	a
55271	.
21143	Garrison
33351	of
66018	Bar
68241	dia
44088	so
18940	far
39619	reduce
60124	ed
07503	by
08208	casualty
55190	s
20683	from
43036	shell
19525	fire
03265	and
06482	bomb
73397	ing
47358	that
60260	it
53187	will
32790	not
60035	be
36768	possible
47843	to
33390	offer
31888	much
40473	resistance
52954	when
17370	enemy
04483	attack
60259	is
28101	launch
60124	ed
55271	.
55091	I
22918	have
21516	given
33705	order
55190	s
47358	that
02870	all
09066	cipher
55190	s
03265	and
42389	secret
15812	document
55190	s
65515	are
47843	to
60035	be

14304	destroy
60124	ed
60019	as
44262	soon
60019	as
04483	attack
05603	begin
55190	s
55271	.
21265	General
66138	Ber
71254	gin
90432	zol
55091	i
99010	10

Message 21 (Starting in Column 60).

20108	For
21265	General
66138	Ber
71254	gin
90432	zol
55091	i
55271	.
54001	You
32021	must
23512	hold
33889	out
60019	as
29045	long
60019	as
36768	possible
55271	.
47430	These
65515	are
68603	Duc
55055	e
55190	s
33705	order
55190	s
55271	.
21265	General
71012	Gal
76254	lin
55019	a
99244	244

Message 22 (Starting in Column 01).

20108	For
21265	General
71012	Gal
76254	lin
55019	a
55271	.
18318	Expect
60124	ed
04483	attack
33558	open
60124	ed
04423	at
13222	dawn
47491	this
31635	morning
55271	.
33933	Outer
13601	defence
55190	s
24724	in
44376	south
52869	west
22918	have
02986	already
05562	been
34086	over
41440	run
07503	by
17370	enemy
46914	tank
55190	s
46295	support
60124	ed
07503	by
25632	infantry
55271	.
08208	Casualty
55190	s
51835	very
23336	high
60019	as
55019	a
40608	result
33351	of
26324	intense
04127	artillery
06488	bombardment
33351	of
20365	forward
13601	defence
55190	s
27418	just
05575	before
13222	dawn
55271	.
02751	Air
04483	attack
55190	s
02988	also
51835	very
23089	heavy
55271	.
21265	General
66138	Ber
71254	gin
90432	zol
55091	i
99016	16

Message 23 (Starting in Column 15).

20108	For
21265	General
66138	Ber
71254	gin
90432	zol
55091	i

55271	.	20431	fourth
55091	I	27093	January
40212	repeat	55271	.
33705	order	54001	You
55190	s	32021	must
33351	of	23512	hold
68603	Duc	33889	out
55055	e	60019	as
48344	transmit	29045	long
84124	ted	60019	as
47843	to	36768	possible
54001	you	55271	.
24724	in	21265	General
32072	my	71012	Gal
47092	telegram	76254	lin
32936	number	55019	a
99244	244	99245	245
33351	of		

Message 24 (Starting in Column 69).

20108	For	05635	being
21265	General	14306	destroyed
71012	Gal	55271	.
76254	lin	65415	Any
55019	a	20922	further
55271	.	30688	message
24308	Imagine	55190	s
60260	it	20683	from
53187	will	54001	you
60035	be	60438	or
38725	quite	60365	me
24596	impossible	53187	will
47843	to	22918	have
23512	hold	47843	to
33889	out	60035	be
31888	much,	42562	sent
29047	longer	24724	in
55271	.	36190	plain
02870	All	27942	language
09066	cipher	55271	.
55190	s	21265	General
03265	and	66138	Ber
42389	secret	71254	gin
15812	document	90432	zol
55190	s	55091	i
65515	are	99017	17
78443	now		

Message 25 (Starting in Column 01).

43553	Situation	04127	artillery
40253	report	03265	and
55271	.	02751	air
18318	Expect	06488	bombardment
60124	ed	55271	.
04483	attack	17370	Enemy
33518	on	46914	tank
66018	Bar	55190	s
68241	dia	46295	support
33558	open	60124	ed
60124	ed	07503	by
04423	at	25632	infantry
13222	dawn	24724	in
47491	this	20128	force
31635	morning	38661	quick
02579	after	60355	ly
18084	exceptional	35361	penetrate
60355	ly	55046	d
42826	severe	33933	outer

13601	defence	10188	communication
55190	s	72019	has
55271	.	05562	been
08208	Casualty	39391	receive
55190	s	55046	d
22918	have	20683	from
05562	been	21265	General
51835	very	66138	Ber
23089	heavy	71254	gin
03265	and	90432	zol
40473	resistance	55091	i
60259	is	43455	since
32790	not	99830	8.30
18318	expect	23790	hour
60124	ed	55190	s
47843	to	55271	.
28029	last	21265	General
51835	very	71012	Gal
29045	long	76254	lin
55271	.	55019	a
32619	No	99246	246

Message 28 (Starting in Column 85).

20040	Following	76254	lin
30688	message	55019	a
39391	receive	55271	.
60124	ed	55091	I
20683	from	22918	have
21265	General	21516	given
66138	Ber	33705	order
71254	gin	55190	s
90432	zol	47843	to
55091	i	08339	cease
04423	at	40473	resistance
99012	12	55271	.
99010	10	21265	General
23790	hour	66138	Ber
55190	s	71254	gin
55271	.	90432	zol
55316	"	55091	i
20108	For	99018	18
21265	General	55325	"
71012	Gal	99247	247

Message 29 (Starting in Column 03).

20108	For	70012	fal
21265	General	76134	len
71012	Gal	55271	.
76254	lin	21265	General
55019	a	65517	Arg
55271	.	69410	ent
72019	Has	73405	ino
66018	Bar	99050	50
68241	dia		

MESSAGES PREFIXED BY 00000

It will be noticed that all but one of these messages are sent from O to N at 12.00 hours, which suggests that they are in the nature of daily reports. When they are compared with the Situation Report messages which are sent out daily at the same hour to CQ from X, it is found that if the check groups and indicators of the latter are omitted, the messages are of the same length. Presumably, therefore, they contain the same text.

When the CQ messages in their basic version are compared carefully with the corresponding 00000 messages and a study is made of repeats in the messages, it will quickly be found that the 00000 messages are recipherments of the CQ message by the use of a conversion table. In this recipherment the second group of the CQ message is put below the first group, the fourth below the third, and so on, and the vertical pairs are then reciphered by the conversion table.

e.g. Message 5 in its basic form opens with the groups

43553 40253 55271 17370

These are set down in the form

43553 55271
40253 17370

and the pairs 44, 30, 52, 55, etc. are reciphered and occupy the same position in the reciphered text as the pairs from which they are derived.

CONVERSION TABLE FOR 00000 MESSAGES

	0	1	2	3	4	5	6	7	8	9
0	34	51	73	99	20	25	09	37	11	06
1	72	08	84	19	21	30	66	63	70	13
2	04	14	41	95	31	05	60	44	81	61
3	15	24	93	80	00	49	50	07	89	52
4	79	22	90	85	27	53	82	91	59	35
5	36	01	39	45	71	88	76	98	62	48
6	26	29	58	17	83	94	16	96	74	92
7	18	54	10	02	68	97	56	86	87	40
8	33	28	46	64	12	43	77	78	55	38
9	42	47	69	32	65	23	67	75	57	03

[It will be noted that the table is reciprocal].

Where a message for recipherment has an odd number of groups, the final group has its digits reciphered by the following digit conversion table, which is also reciprocal.

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

MESSAGE 10

2nd Process	47039	87057	59500	40452	22773	22772
	47124	81440	37134	95726	33306	33306
1st Process	28596	55271	47092	32936	99015	99016
	76135	54018	55190	55190	55280	55280
Clear Text	Lt. Col. Leo	. Your	telegram	number s	15 ,	16 ,
2nd Process	43769	30912	92842	63306	00203	89546
	22367	23938	45442	18447	55463	03256
1st Process	99017	99018	60124	28029	22308	33351
	03265	39391	55271	99006	55190	32936
Clear Text	17 and	18 receive	ed .	Last 6	group s	of number
2nd Process	62701	47957	52461	63029	93272	11364
	93387	56542	35134	00598	62725	
1st Process	99016	55271	40212	21265	69410	99046
	25213	36310	55271	65517	73405	
Clear Text	16 indeci-pher-able	. Please	repeat .	General Arg	ent ino	46

S. Inspection of the messages reveals that the final group of a message is often of a distinctive pattern, e.g. Messages 1 and 2 end respectively with the groups 46565 and 72424. It looks as though the final two digits in each case are nulls added to complete a 5-figure group. If this is so, it means that the length of the two messages are 93 and 63 digits respectively. From this it is clear that the unit of substitution is 3-figures. This conclusion can also be reached by a study of the length of inter-message repeats.

The messages are then analysed for recurrences between them in order that they may be set correctly in depth. It may not be possible to set all messages by these means, but from the large number which can be set it becomes apparent that the starting point of each message is governed by the hour of origin, e.g. Messages 1 and 20 with time of origin 04 and 16 hours respectively start in column 1, Messages 3 and 21 with hours of origin 05 and 17 hours respectively start in column 2. The subtractor is non-recurring.

When all the messages have been set in depth, examination is made for limitations. It is found that the first digits of groups in any column are limited to a maximum of 6, and these run consecutively. Indeed in the majority of columns there are only 5 first digits. From this we may assume that the book groups run from 000 to 599, and that the groups 500-599 are uncommon.

Use is now made of the limitation to obtain subtractors for the first digits of every column in which there is sufficient depth. An example of this is given below.

	6 7 . .	2 . .	4 . .	1 . .	4 . .	6 . .	2 . .	5 . .	0 . .
1.	0 4 5 4 3	6 0 0 4	4 5 8 0	2 9 8 1	7 0 7 3	6 1 7 0	5 2 6 3	9 0 1 4	4 8 4 4
3.		2 3 9 0	8 3 0 4	1 5 5 0	8 8 3 4	6 2 2 0	5 0 6 3	5 0 7 0	1 9 1 1
5.			8 7 5 4	5 7 8 4	4 6 5 0	7 3 6 1	5 2 5 3	5 1,2 0	3 7 4 3
6.			4 6 0 0	5 7 7 4	4 2 5 0	0 3 6 4	5 8 9 3	8 5 7 3	4 0 7 4
7.				1 6 9 0	4 2 4 0	1 2 6 5	2 3 3 0	5 4 6 0	0 4 5 0
20.	7 1 6 1 0	5 2 5 3	6 2 5 2	1 6 2 0	8 0 4 4	9 3 1 3	5 6 9 3	9 0 6 4	0 5 1 0
23.		2 9 1 0	4 1 7 0	6 4 8 5	6 4 2 2	6 0 3 0	6 4 1 4	0 5 1 5	3 5 4 3
24.			8 7 5 4	5 7 8 4	4 6 5 0	7 3 6 1	4 6 5 2	5 2 3 0	1 8 9 1

These basic first digits can now be used to reveal latent inter-message repeats, e.g. From the basic first digits of groups in the above messages the following assumptions may be made,

(i) Messages 1 and 5 start with the same 7 groups.

(ii) Message 24 starts the same as Message 1 for the first 4 groups.

(iii) If (i) and (ii) are correct, the first digit of Message 1 must be 4, i.e. the digit of the subtractor at that point is 6, not 7.

(iv) Messages 3 and 6 start with the same 4 groups. (Actually this is incorrect as only the first 3 groups are the same).

(v) Messages 7 and 23 start with the same 3 groups. (This again is incorrect as only the first 2 groups are the same).

Let us assume a Provisional Subtractor of 600 for column 1; then Message 1 begins with the group 445. By assumption (i) above Message 5 also starts with the group 445. Hence the Provisional Subtractor for column 3 must be 430. This gives us 028 as the third group of Message 1 and by applying this information to Message 5 we obtain a Provisional Subtractor 447 for column 5. Similarly we can obtain Provisional Subtractors for columns 7 and 9.

We now know that the second group of Message 3 is 400. By assumption (iv) above the second group of Message 6 must also be 400, i.e. the Provisional Subtractor for column 4 must be 177. This in its turn gives us the second group of Message 24 and the fourth group of Message 1, enabling us to get Provisional Subtractors for columns 2 and 6. Naturally it will not be possible to obtain Provisional Subtractors for all the columns by this method, but a sufficient number can be found to enable us to start breaking the text.

Below are shown the Provisional Subtractors and Base for the messages set out in the table above.

	600	209	430	177	447	615	265	510	013
1.	045	600	458	298	707	617	526	901	484
	445	401	028	121	360	002	361	491	471
3.		239	830	155	883	622	506	507	191
		030	400	088	446	017	341	-097	188
5.			875	578	465	736	525	512	374
			445	401	028	121	360	002	361
6.			460	577	425	036	589	857	407
			030	400	088	421	324	347	494
7.				169	424	126	233	546	045
				092	087	511	078	036	032
20.	716	525	625	162	804	931	569	906	051
	116	326	295	095	467	326	304	496	048
23.		291	417	648	642	603	641	051	354
		092	087	571	205	098	486	541	341
24.			875	578	465	736	465	523	189
			445	401	028	121	200	013	176

The limitation on the number of groups suggests that there may be a bigram base. If this is so, the long repeat between Messages 1 and 2 might well start with

445 401 028 121 360 002 361 491 471 -
SI TU AT IO NR EP OR TS TO P -

The values NR = 360, OR = 361 immediately strike the eye. Consider also the values

TO = 471
TS = 491
TU = 401

S is 4 letters on in the alphabet from O, U is 2 letters further on than S. The corresponding intervals between the code groups are 20 and 10. This at once suggests

TO	471
TP	476
TQ	481
TR	486
TS	491
TT	496
TU	401

From this and from the values already noted

NR	360
OR	361

the broad outlines of the basic bigram table become apparent.

Let us assume that AA = 000, then AT = 095. In our Provisional Base AT = 028; therefore, a further subtractor of 033 may well bring us to true base. Unfortunately, however, we quickly find that this is not so. Our bigram table we have assumed to be constructed on the following principles:-

2ND LETTER OF PAIR

1ST LETTER OF PAIR	A	B	C	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	000	005	010	065	070	075	080	085	090	095	100	105	110	115	120	125
B	001															126
C	002															127
D	003															128
E	004															129
F	130	135	140	195	200	205	210	215	220	225	230	235	240	245	250	255
G	131															256
H	132															257
I	133															258
J	134															259
K	260	265	270	325	330	335	340	345	350	355	360	365	370	375	380	385
L	261															386
M	262															387
N	263															388
O	264															389
P	390															

By applying a further subtractor of 033 to the Provisional Base of Message 1, we obtain the following values:-

412 478 095 198 337 079 338 468 448

SI TU AT IO NR EP OR TS TO

Comparing these values with those to be found in the table above, we naturally find that AT is correct, because it was on the value for this pair that we based the figure for our further subtractor. The value for EP also is correct. The value for IO, however, is given in the table as 203, whereas in actual fact in the message it is 198. This must mean that between the values for EP and IO 5 bigrams have been omitted in the basic table. Looked at from another aspect, it probably means that one of the letters in the top row of the table has been omitted. Furthermore, in the table NR has the value 348, whereas in the message it appears as 337. If, however, we omit a letter from the top line of our table and also from the letters at the side, we shall be able to give NR the value 337. It is very probable that the letter which has to be omitted in both cases is the same letter. In the case of the side column the omitted letter must fall between I and N. Clearly the most probable letter is J, and if we assume that this is so, then AT becomes not 095, but 090, i.e. the further subtractor required will be 038, not 033. When this is applied throughout the text and a table constructed on the same lines as that shown above, but with the letter J omitted, it is found that the messages can be solved.

SUBTRACTOR

638	237	468	105	475	643	293	548	041	347
629	896	808	271	684	513	280	602	735	812
524	695	176	324	159	252	823	792	670	713
136	554	413	708	459	965	073	943		

STARTING POINT SYSTEM

Hour of Origin	04 16	05 17	06 18	07 19	08 20	09 21	10 22	11 23	12 00	13 01	14 02	15 03
Start in Column	1	2	3	4	5	6	7	8	9	10	11	12

BASIC BIGRAM TABLE

1ST LETTER										
	A	B	C	D	E	0	25	50	75	100
	F	G	H	I	K	125	150	175	200	225
	L	M	N	O	P	250	275	300	325	350
	Q	R	S	T	U	375	400	425	450	475
	V	W	X	Y	Z	500	525	550	575	600
	0	1	2	3	4	A	F	L	Q	V
	5	6	7	8	9	B	G	M	R	W
	10	11	12	13	14	C	H	N	S	X
	15	16	17	18	19	D	I	O	T	Y
	20	21	22	23	24	E	K	P	U	Z

2ND LETTER

e.g. ER = 75 + 9 = 84; ND = 250 + 17 = 267.

Clear text of the messages.

1. SITUATION REPORT STOP. COUNTER ATTACK CARRIED OUT BY FRESH ITALIAN TROOPS.

2. SITUATION REPORT STOP. COUNTER ATTACK BEATEN OFF(Q).

3. CASUALTIES ONE OFFICER KILLED, ONE WOUNDED; OTHER RANKS SEVENTEEN WOUNDED.

4. TWELVE PRISONERS TAKEN INCLUDING ONE OFFICER(X).

5. SITUATION REPORT: FORWARD TRENCHES SHELLED FOR HALF AN HOUR.

6. CASUALTY REPORT: OFFICERS NIL, OTHER RANKS THREE WOUNDED(X).

7. ENEMY RAID BEATEN OFF, ONE MAN MISSING(X).

8. OPERATIONS ORDER FOR ATTACK NOT YET RECEIVED.

9. YOUR OPERATIONS ORDER NUMBER NINETEEN HAS BEEN RECEIVED.

10. ENEMY BARRAGE ON FORWARD TRENCHES HAS BEGUN AGAIN.

11. CASUALTIES: SIX OTHER RANKS KILLED AND TWENTY TWO WOUNDED.

12. BARRAGE CONTINUES; CASUALTIES MOUNTING.

13. BARRAGE HAS LIFTED TO SUPPORT TRENCHES(X).

14. MASS TANKS ADVANCING SUPPORTED BY INFANTRY(Q).

15. PRESSURE VERY HEAVY; SEND REINFORCEMENTS(X).

16. HOLDING ON BUT CASUALTIES VERY HEAVY; SEND REINFORCEMENTS(X).

17. POSITION STILL DIFFICULT; RETIREMENT ORDERED TO SUPPORT TRENCHES.

18. SITUATION REPORT: HALF MY FORCE CASUALTIES.

19. TANKS HAVE CROSSED FRONT TRENCHES EVERYWHERE(Q).

20. INTEND COUNTER ATTACK IMMEDIATELY ON ARRIVAL REINFORCEMENTS(X).

21. UNLESS REINFORCEMENTS ARRIVE SOON IT WILL BE IMPOSSIBLE ORGANISE ATTACK.

22. TWO PLATOONS B COMPANY NOW REPORTED ARRIVED(X).

23. ENEMY INFANTRY CONSOLIDATING OUR FRONT LINE.

24. SITUATION EASIER, COUNTER ATTACK NOW BEING ORGANISED(Q).

25. HAVE ORGANISED MY COUNTER ATTACK FOR NINETEEN HUNDRED HOURS(Q).

26. HAVE ARRANGED WITH DIVISIONAL ARTILLERY FOR CREEPING BARRAGE(X).

27. ENEMY SHELLING HAS PRACTICALLY CEASED(X).

28. CASUALTY REPORT: OFFICERS WOUNDED ELEVEN, KILLED AND MISSING SEVEN.

29. CASUALTY REPORT: TOTAL NUMBER OTHER RANKS KILLED FORTY NINE AND WOUNDED NINETY FIVE.

30. A PLATOON HAS RECAPTURED OUR FORWARD TRENCHES IN C SECTOR.

31. FOURTEEN ENEMY OTHER RANKS HAVE BEEN TAKEN PRISONER PLUS TWO WOUNDED OFFICERS.

32. REMAINDER OF FRONT LINE NOW REGAINED AND BEING CONSOLIDATED(Q).

33. RECOMMEND LIEUT. COLONEL PUFFIN FOR D.S.O. FOR GALLANTRY STOP. PUFFIN LT. COL.

T. A certain number of the messages can be set in depth by means of inter-message recurrences, e.g. In messages 5 and 8 the groups 4838 3030 occur consecutively. Further, it will be noted that message 6 begins 4838 2119 3030, which suggests that the group 2119 is an Indicator. Confirmation of this comes from the fact that in message 5 the groups 4949 4064 occur, and message 21 begins 4949 9293 4064.

When as many messages as possible have been set in depth, a study of the columns obtained reveals that they conform to the limitation found when all groups of the basic book consist either of odd digits or of even digits [see Section V, Exercise 1 (ii)]. By use, therefore, of this limitation all the messages can be set in depth.

It now becomes apparent that the subtractor consists of 100 groups, and that not only the second group in each message, but also the penultimate group is an Indicator.

METHOD OF OBTAINING A PROVISIONAL BASE

It will be noted that in every case in which two messages end in the same column the last groups of those messages are the same. It may be assumed, therefore, that every message ends with the same group, which probably represents STOP.

If we assume that in our Provisional Base the group for STOP is 0000, we can at once reduce to that Provisional Base all columns in which there is the last group of a message, i.e. 15 columns in all.

Difference tables for these columns should now be made, and a list compiled of those differences which occur most frequently. When this has been done, Difference tables must be made for other columns and the results compared with the list of common differences. Owing to the limitation of the book, many spurious differences will be thrown up, and it will frequently be difficult to decide which one of several subtractors is the correct one. In such cases the subtractor which produces the most common groups should be chosen, even though it may in the end prove to be wrong.

After a certain number of columns have been reduced to a Provisional Base, further limitations of the book will become apparent, and these may be used to decide in cases where the Difference Tables produce more than one possible subtractor, which in actual fact is the correct one. These further limitations are three in number: (i) limitation on the first digit; (ii) limitation on the first pair of digits; (iii) limitation on the second pair of digits. The appearance which these limitations assumes in a Provisional Base founded on the assumption that 0000 = STOP, are (i) 4 does not occur as a first digit; (ii) the following first pairs of digits do not occur 02, 13, 24, 35, 46, 57, 68, 79, 80, 91; (iii) the following second pairs of digits do not occur 04, 15, 26, 37, 48, 59, 60, 71, 82, 93.

If we now assume that there are two separate tables, one of odd groups, the other of even groups, we find that owing to the limitation only 400 odd groups are possible and only 320 even groups. Such a small number of groups, 720 in all, excludes the possibility of a dictionary as the base and leads to the assumption that the base is syllabic. It is now noticed that if we exclude the vowels from the alphabet and construct a Consonant Bigram Table, such a table would consist of exactly 400 bigrams. Furthermore, if we then construct a Table of bigrams in which vowels occur, we shall have a table of 276 bigrams. If we add to this table a single letter alphabet, we increase the number of groups to 302 and may assume that the 18 groups required to bring the number to 320 represent punctuation marks and, perhaps, digits.

It seems probable that the limitations observed in our Provisional Base will in the True Base appear in the form that doubled digits (00, 11, 22 etc.) do not occur as first or second pairs of groups, and that the particular digit which does not occur as the first of a group will be either 0 or 9.

A process of experiment with the text will enable us to reconstruct the Plain Text and the original tables.

TABLE I

1st PAIRS \ 2nd PAIRS	02	04	06	08	20	24	26	28	40	42	46	48	60	62	64	68	80	82	84	86
02	BB	BC	BD	BF	BG	BH	BJ	BK	BL	BM	BN	BP	BQ	BR	BS	BT	BV	BW	BX	BZ
04	CB	CC	CD	CF	CG	CH	CJ	CK	CL	CM	CN	CP	CQ	CR	CS	CT	CV	CW	CX	CZ
06	DB	DC	DD	DF	DG	DH	DJ	DK	DL	DM	DN	DP	DQ	DR	DS	DT	DV	DW	DX	DZ
08	FB	FC	FD	FF	FG	FH	FJ	FK	FL	FM	FN	FP	FQ	FR	FS	FT	FV	FW	FX	FZ
20	GB	GC	GD	GF	GG	GH	GJ	GK	GL	GM	GN	GP	GQ	GR	GS	GT	GV	GW	GX	GZ
24	HB	HC	HD	HF	HG	HH	HJ	HK	HL	HM	HN	HP	HQ	HR	HS	HT	HV	HW	HX	HZ
26	JB	JC	JD	JF	JG	JH	JJ	JK	JL	JM	JN	JP	JQ	JR	JS	JT	JV	JW	JX	JZ
28	KB	KC	KD	KF	KG	KH	KJ	KK	KL	KM	KN	KP	KQ	KR	KS	KT	KV	KW	KX	KZ
40	LB	LC	LD	LF	LG	LH	LJ	LK	LL	LM	LN	LP	LQ	LR	LS	LT	LV	LW	LX	LZ
42	MB	MC	MD	MF	MG	MH	MJ	MK	ML	MM	MN	MP	MQ	MR	MS	MT	MV	MW	MX	MZ
46	NB	NC	ND	NF	NG	NH	NJ	NK	NL	NM	NN	NP	NQ	NR	NS	NT	NV	NW	NX	NZ
48	PB	PC	PD	PF	PG	PH	PJ	PK	PL	PM	PN	PP	PQ	PR	PS	PT	PV	PW	PX	PZ
60	QB	QC	QD	QF	QG	QH	QJ	QK	QL	QM	QN	QP	QQ	QR	QS	QT	QV	QW	QX	QZ
62	RB	RC	RD	RF	RG	RH	RJ	RK	RL	RM	RN	RP	RQ	RR	RS	RT	RV	RW	RX	RZ
64	SB	SC	SD	SF	SG	SH	SJ	SK	SL	SM	SN	SP	SQ	SR	SS	ST	SV	SW	SX	SZ
68	TB	TC	TD	TF	TG	TH	TJ	TK	TL	TM	TN	TP	TQ	TR	TS	TT	TV	TW	TX	TZ
80	VB	VC	VD	VF	VG	VH	VJ	VK	VL	VM	VN	VP	VQ	VR	VS	VT	VV	VW	VX	VZ
82	WB	WC	WD	WF	WG	WH	WJ	WK	WL	WM	WN	WP	WQ	WR	WS	WT	WV	WW	WX	WZ
84	XB	XC	XD	XF	XG	XH	XJ	XK	XL	XM	XN	XP	XQ	XR	XS	XT	XV	XW	XX	XZ
86	ZB	ZC	ZD	ZF	ZG	ZH	ZJ	ZK	ZL	ZM	ZN	ZP	ZQ	ZR	ZS	ZT	ZV	ZW	ZX	ZZ

TABLE II

1st PAIRS \ 2nd PAIRS	13	15	17	19	31	35	37	39	51	53	57	59	71	73	75	79	91	93	95	97
13	AA	AE	AI	AO	AU	AY	BA	BE	BI	BO	BU	BY	CA	CE	CI	CO	CU	CY	DA	DE
15	DI	DO	DU	DY	EA	EE	EI	EO	EU	EY	FA	FE	FI	FO	FU	FY	GA	GE	GI	GO
17	GU	GY	HA	HE	HI	HO	HU	HY	IA	IE	II	IO	IU	IY	JA	JE	JI	JO	JU	JY
19	KA	KE	KI	KO	KU	KY	LA	LE	LI	LO	LU	LY	MA	ME	MI	MO	MU	MY	NA	NE
31	NI	NO	NU	NY	OA	OE	OI	OO	OU	OY	PA	PE	PI	PO	PU	PY	QA	QE	QI	QO
35	QU	QY	RA	RE	RI	RO	RU	RY	SA	SE	SI	SO	SU	SY	TA	TE	TI	TO	TU	TY
37	UA	UE	UI	UO	UU	UY	VA	VE	VI	VO	VU	VY	WA	WE	WI	WO	WU	WY	XA	XE
39	XI	XO	XU	XY	YA	YE	YI	YO	YU	YY	ZA	ZE	ZI	ZO	ZU	ZY	A	B	C	D
51	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
53	Y	Z	.	,	(	)	"	"	-	:	;	AND	BUT	DID	HAVE	HAS	HAD	NOT	THE	WAS
57	AB	AC	AD	AF	AG	AH	AJ	AK	AL	AM	AN	AP	AQ	AR	AS	AT	AV	AW	AX	AZ
59	EB	EC	ED	EF	EG	EH	EJ	EK	EL	EM	EN	EP	EQ	ER	ES	ET	EV	EW	EX	EZ
71	IB	IC	ID	IF	IG	IH	IJ	IK	IL	IM	IN	IP	IQ	IR	IS	IT	IV	IW	IX	IZ
73	OB	OC	OD	OF	OG	OH	OJ	OK	OL	OM	ON	OP	OQ	OR	OS	OT	OV	OW	OX	OZ
75	UB	UC	UD	UF	UG	UH	UJ	UK	UL	UM	UN	UP	UQ	UR	US	UT	UV	UW	UX	UZ
79	YB	YC	YD	YF	YG	YH	YJ	YK	YL	YM	YN	YP	YQ	YR	YS	YT	YV	YW	YX	YZ

TABLE III. THE SUBTRACTOR

00	01	02	03	04	05	06	07	08	09
1370	6658	0125	7076	9108	4245	5571	1004	2362	1240
10	11	12	13	14	15	16	17	18	19
5195	8371	4628	4945	1336	2848	7541	9416	6104	5058
20	21	22	23	24	25	26	27	28	29
4567	2211	0300	3587	3859	4247	5153	6281	7476	9999
30	31	32	33	34	35	36	37	38	39
8123	5697	4414	8093	1755	8655	8001	9193	7462	1145
40	41	42	43	44	45	46	47	48	49
3086	1250	3459	8114	6576	0104	5678	9214	5764	3334
50	51	52	53	54	55	56	57	58	59
4333	4675	4129	8765	4010	6756	4118	9543	0521	6803
60	61	62	63	64	65	66	67	68	69
5411	2647	3919	1008	5568	5571	3908	4144	7965	3218
70	71	72	73	74	75	76	77	78	79
9999	6747	1826	3515	7424	9583	7853	0030	1122	7654
80	81	82	83	84	85	86	87	88	89
8505	4016	6149	1457	8482	6331	5494	8264	1738	5915
90	91	92	93	94	95	96	97	98	99
0421	2632	4001	1755	5424	8019	6707	5210	8566	0731

[Note that the second 50 groups of the Subtractor are the exact reversal of the first 50 groups].

TABLE IV. BASIC GROUPS AND PLAIN TEXT

Text 1. (Starting in Column 06).

5395	The	3519	re	4840	pl
1397	de	6464	ss	5715	ac
1337	ba	5757	an	5113	e
3579	te	5959	ep	3115	no
8224	wh	7179	it	5173	r
7115	ic	7353	om	1379	co
5119	h	5113	e	7557	un
5957	en	7319	of	3553	se
3571	su	5395	the	5139	l
5917	ed	1379	co	5397	was
5397	was	7573	ur	1937	la
7157	in	3553	se	0428	ck
7179	it	7319	of	7157	in
5175	s	1951	li	5117	g
6404	sc	1559	fe	7157	in
7359	op	5317	.	1513	di
5113	e	1997	Ne	2046	gn
5359	and	7179	it	7179	it
4862	pr	1719	he	5313	y
7331	og	5173	r	5317	.

The debate which ensued was in its scope and progress an epitome of the course of life. Neither place nor counsel was lacking in dignity.

Text 2. (Starting in Column 27)

5395	The	6264	rs	1915	ke
1397	de	3773	we	5957	en
1337	ba	3519	re	5975	es
3579	te	5395	the	5179	t

7157	in	3773	we	1753	ie
5395	the	3519	re	6468	st
1937	la	5957	en	5359	and
4606	nd	1591	ga	1979	mo
5319	,	1593	ge	6468	st
5395	the	3997	d	3751	vi
5395	the	7357	on	3575	ta
1973	me	5395	the	5139	l
5395	the	1953	lo	5317	.
5313	y	0868	ft		

The debaters were the keenest in the land, the theme they were engaged on the loftiest and most vital.

Text 3. (Starting in Column 06).

5395	The	4862	pr	0240	bl
1731	hi	5975	es	7175	is
2024	gh	5957	en	2442	hm
1717	ha	3575	ta	5957	en
4040	ll	3591	ti	5179	t
7319	of	3739	ve	5991	ev
1735	Ho	5359	and	5973	er
6246	rn	3559	so	1951	li
5975	es	3737	va	6468	st
1735	ho	3531	ri	5957	en
7575	us	5917	ed	5917	ed
5113	e	3115	no	3593	to
5391	had	5173	r	3991	a
1997	ne	5391	had	1937	la
3739	ve	5395	the	4620	ng
5173	r	7351	ol	3713	ua
1339	be	3997	d	1593	ge
1719	he	3517	ra	3559	so
4006	ld	0868	ft	5957	en
5757	an	5973	er	1393	cy
5775	as	5175	s	0440	cl
3553	se	7319	of	7359	op
4202	mb	6824	th	1315	ae
1959	ly	5779	at	1513	di
3559	so	5975	es	3995	c
3519	re	3575	ta	5317	.

The high hall of Horne's house had never beheld an assembly so representative and so varied nor had the old rafters of that establishment ever listened to a language so encyclopaedic.

Text 4. (Starting in Column 00).

3991	A	6404	sc	7579	ut
1591	ga	5957	en	5119	h
4040	ll	5113	e	7179	it
5757	an	7157	in	1971	ma
5179	t	6862	tr	1397	de
				5317	.

A gallant scene in truth it made.

Text 5. (Starting in Column 52).

0462	Cr	1573	fo	5175	s
7379	ot	7379	ot	6468	st
5395	the	7319	of	3531	ri
6264	rs	5395	the	1917	ki
5397	was	3575	ta	4620	ng
5395	the	0240	bl	1731	hi
3519	re	5113	e	2024	gh
5779	at	7157	in	1937	la
5395	the	1731	hi	4606	nd

1591	ga	5117	g	5395	the
6202	rb	0862	fr	1991	Mu
5319	,	7353	om	4040	ll
1731	hi	5395	the	7319	of
5175	s	0262	br	1591	Ga
1557	fa	7157	in	4040	ll
1373	ce	5313	y	7393	ow
2040	gl	1317	ai	1335	ay
7393	ow	6264	rs	5317	.
7157	in	7319	of		

Crotthers was there at the foot of the table in his striking highland garb, his face glowing from the briny airs of the Mull of Galloway.

Text 6. (Starting in Column 57).

5395	The	5113	e	1531	ea
3519	re	1379	co	6240	rl
3593	to	7557	un	5313	y
5157	o	3579	te	1397	de
5319	,	1995	na	4862	pr
7359	op	4604	nc	5791	av
3173	po	5113	e	7179	it
3557	si	1353	bo	5313	y
3579	te	3519	re	5359	and
3593	to	5751	al	4862	pr
1731	hi	3519	re	5953	em
5151	m	5717	ad	5779	at
5397	was	5313	y	7573	ur
1959	Ly	5395	the	5113	e
4604	nc	6468	st	3775	wi
5119	h	7131	ig	6406	sd
5319	,	1971	ma	7353	om
8224	wh	3575	ta	5317	.
7375	os	7319	of		

There too, opposite to him was Lynch, whose countenance bore already the stigmata of early depravity and premature wisdom.

Text 7. (Starting in Column 04).

1997	Ne	5951	el	5779	at
8468	xt	1953	lo	5917	ed
5395	the	5319	,	7157	in
6404	Sc	5395	the	6468	st
7379	ot	5915	ec	7351	ol
0424	ch	1373	ce	7117	id
1971	ma	4668	nt	3519	re
5153	n	3531	ri	3173	po
5397	was	3995	c	3553	se
5395	the	5319	,	5395	the
4840	pl	8224	wh	6460	sq
5715	ac	7151	il	3713	ua
5113	e	5113	e	5179	t
5775	as	5779	at	1573	fo
3557	si	1731	hi	6242	rm
2046	gn	5175	s	7319	of
5917	ed	3557	si	1971	Ma
3593	to	1397	de	0606	dd
1379	Co	5397	was	5957	en
6468	st	3553	se	5317	.

Next the Scotchman was the place assigned to Costello, the eccentric, while at his side was seated in stolid repose the squat form of Madden.

Text 8. (Starting in Column 52).

5395	The	3519	re	4840	pl
0424	ch	7319	of	5313	y
1317	ai	1337	Ba	3775	wi
5173	r	4646	nn	6824	th
7319	of	7357	on	5395	the
5395	the	7157	in	4862	pr
3519	re	5995	ex	7153	im
3557	si	4840	pl.	3535	ro
1397	de	7373	or	3553	se
4668	nt	5973	er	5951	el
7157	in	5175	s	5931	eg
1397	de	1917	ki	5757	an
5917	ed	5179	t	1373	ce
6468	st	7319	of	5359	and
3139	oo	6882	tw	3593	to
3997	d	1535	ee	8246	wn
3737	va	3997	d	0262	br
1371	ca	6424	sh	5917	ed
4668	nt	7373	or	1971	ma
1339	be	6864	ts	4646	nn
1573	fo	5359	and	5973	er
3519	re	3551	sa	5175	s
5395	the	4068	lt	7319	of
1719	he	5917	ed	1971	Ma
5773	ar	1379	co	1937	la
6824	th	8224	wh	0424	ch
5371	but	7117	id	5131	i
7357	on	5113	e	3535	Ro
1537	ei	0262	br	1937	la
5395	the	7331	og	4606	nd
5173	r	3715	ue	6468	St
0840	fl	5175	s	1793	Jo
5757	an	1379	co	2446	hn
5137	k	4668	nt	1991	Mu
7319	of	3517	ra	4040	ll
7179	it	6468	st	7131	ig
5395	the	5917	ed	5757	an
1571	fi	6424	sh	5317	.
1713	gu	5773	ar		

The chair of the resident indeed stood vacant before the hearth but on either flank of it the figure of Bannon in explorer's kit of tweed shorts and salted cowhide brogues contrasted sharply with the primrose elegance and town bred manners of Malachi Roland St. John Mulligan.

Text 9. (Starting in Column 00).

5395	The	5151	m	7153	im
6468	st	3991	a	3173	po
3517	ra	6440	sl	3553	se
4620	ng	7393	ow	3997	d
5973	er	3519	re	5319	,
6468	st	1373	ce	5775	as
7151	il	6464	ss	7179	it
5139	l	1759	io	3553	se
3519	re	5153	n	5953	em
1591	ga	7319	of	5917	ed
6206	rd	6824	th	5319	,
5917	ed	5779	at	1359	by
7357	on	1557	fa	1717	ha
5395	the	4064	ls	1351	bi
1557	fa	5113	e	5179	t
1373	ce	1371	ca	7373	or
1339	be	4042	lm	3559	so
1573	fo	5395	the	1973	me
3519	re	3519	re	6468	st
1731	hi	5319	,	7517	ud

1753	ie	5715	ac	3991	a
3997	d	1391	cu	0840	fl
6862	tr	3553	se	1317	ai
7115	ic	7157	in	5173	r
5137	k	5395	the	5319	,
5319	,	7173	ir	1573	fo
7559	up	6448	sp	5173	r
7357	on	1531	ea	5395	the
3779	wo	1915	ke	0462	cr
6206	rd	5173	r	7517	ud
5175	s	5757	an	5973	er
3559	so	7557	un	6824	th
5953	em	1719	he	7157	in
1351	bi	5751	al	2064	gs
6868	tt	6824	th	7319	of
5973	er	7157	in	1951	li
5917	ed	5975	es	1559	fe
5775	as	5175	s	5317	.
3593	to	5319	,		

The stranger still regarded on the face before him a slow recession of that false calm there, imposed, as it seemed, by habit or some studied trick, upon words so embittered as to accuse in their speaker an unhealthiness, a flair, for the cruder things of life.

Text 10. (Starting in Column 67).

3991	A	3553	se	4862	pr
6404	sc	5953	em	5975	es
5957	en	5319	,	5957	en
5113	e	1359	by	5179	t
1513	di	3991	a	5395	the
3553	se	3779	wo	3519	re
4620	ng	6206	rd	5331	(
5731	ag	7319	of	5775	as
5975	es	3559	so	3559	so
7179	it	1995	na	1973	me
3553	se	3595	tu	6824	th
4008	lf	3517	ra	3151	ou
7157	in	5139	l	2024	gh
5395	the	3991	a	5179	t
7313	ob	1735	ho	5335	)
3553	se	1973	me	3775	wi
6280	rv	1951	li	6824	th
5973	er	1997	ne	5395	the
5175	s	6464	ss	7173	ir
1973	me	5775	as	7153	im
1979	mo	7119	if	1973	me
3539	ry	6824	th	1513	di
5319	,	7375	os	5779	at
5991	ev	5113	e	5113	e
7339	ok	1395	da	4840	pl
5917	ed	7975	ys	1531	ea
5319	,	3773	we	3571	su
7179	it	3519	re	3519	re
3779	wo	3519	re	5175	s
7551	ul	5751	al	5317	.
3997	d	1959	ly		

A scene disengages itself in the observer's memory, evoked, it would seem, by a word of so natural a homeliness as if those days were really present there (as some thought) with their immediate pleasures.

Text 11. (Starting in Column 27).

1971	Ma	6268	rt	1973	me
6228	rk	1719	he	4202	mb
6824	th	5173	r	5973	er
7175	is	5359	and	5317	.
1557	fa	3519	re		

Mark this farther and remember.

Text 12. (Starting in Column 09).

5395	The	1973	me	5957	en
5957	en	5175	s	1959	ly
3997	d	3571	su	5317	.
1379	co	0606	dd		

The end comes suddenly.

Text 13. (Starting in Column 00).

5957	En	6268	rt	3553	se
3579	te	5119	h	4202	mb
5173	r	8224	wh	1939	le
6824	th	5973	er	3997	d
5779	at	5113	e	5359	and
5757	an	5395	the	5393	not
3579	te	6468	st	5113	e
0424	ch	7517	ud	5395	the
5753	am	1759	io	7173	ir
1339	be	7575	us	1557	fa
5173	r	5773	ar	1373	ce
7319	of	5113	e	5175	s
1351	bi	5775	as	5317	.

Enter that ante-chamber of birth where the studious are assembled and note their faces.

Text 14. (Starting in Column 69).

5393	Not	5953	em	6424	sh
1731	hi	5175	s	7373	or
4620	ng	5319	,	3751	vi
5319	,	5395	the	7351	ol
5775	as	3519	re	5957	en
7179	it	7319	of	5179	t
3553	se	3517	ra	5317	.

Nothing, as it seems, there of rash or violent.

Text 15. (Starting in Column 00).

7357	On	5137	k	5319	,
3771	wa	5319	,	5395	the
6206	rd	7557	un	3551	sa
3593	to	6440	sl	4068	lt
5395	the	5739	ak	7157	in
1397	De	5917	ed	5995	ex
5717	ad	5359	and	1717	ha
3553	Se	3775	wi	7575	us
3991	a	6824	th	3591	ti
5395	the	1735	ho	0240	bl
5313	y	6262	rr	5113	e
6862	tr	7113	ib	0840	fl
5753	am	1939	le	3139	oo
5159	p	1713	gu	3997	d
3593	to	4048	lp	5317	.
0662	dr	7157	in		
7157	in	2064	gs		

Onward to the Dead Sea they tramp to drink, unslaked and with horrible gulpings, the salt inexhaustible flood.

Text 16. (Starting in Column 00).

5359	And	1971	ma	1995	na
5395	the	2046	gn	5313	y
5971	eq	7119	if	3593	to
3717	ui	1753	ie	1719	he
1997	ne	3997	d	5791	av
3173	po	7157	in	5957	en
6268	rt	5395	the	5175	s
5957	en	1397	de	7393	ow
5179	t	3553	se	5153	n
2062	gr	6268	rt	1971	ma
7393	ow	5917	ed	2046	gn
5175	s	1719	he	7179	it
5731	ag	5791	av	7517	ud
1317	ai	5957	en	5113	e
5153	n	5175	s	5317	.
5319	,	5319	,		

And the equine portent grows again, magnified in the deserted heavens, nay to heaven's own magnitude.

Text 17. (Starting in Column 12).

3771	Wa	7319	of	3551	sa
6468	st	6404	sc	4606	nd
5113	e	3519	re	0240	bl
1937	la	5915	ec	7157	in
4606	nd	1735	ho	3997	d
5319	,	8240	wl	7559	up
3991	a	5175	s	7559	up
1735	ho	5359	and	3991	a
1973	me	5395	the	5317	.

Waste land, a home of screech owls and the sand blind upupa.

Text 18. (Starting in Column 15).

5379	Has	5775	as	1997	ne
1719	he	1719	he	1571	fi
1573	fo	1573	fo	6864	ts
6220	rg	6220	rg	3519	re
7379	ot	5979	et	1373	ce
3579	te	5175	s	7191	iv
5153	n	5751	al	5917	ed
6824	th	5139	l	5317	.
7175	is	1339	be		

Has he forgotten this as he forgets all benefits received.

Text 19. (Starting in Column 17).

5379	Has	5951	el	3771	wa
1719	he	3997	d	4668	nt
5393	not	6824	th	7319	of
1997	ne	5779	at	3991	a
5773	ar	1951	li	4840	pl
5973	er	5975	es	3151	ou
1735	ho	1557	fa	2024	gh
1973	me	4040	ll	6424	sh
3991	a	7393	ow	5773	ar
3553	se	1573	fo	5113	e
5917	ed	5173	r	5317	.
1571	fi	5395	the		

Has he not nearer home a seed field that lies fallow for the want of a ploughshare.

Text 20. (Starting in Column 69).

7179	It	1731	hi	5779	at
7151	il	5151	m	1597	go
5139	l	3593	to	6448	sp
1339	be	4862	pr	5951	el
1379	co	1531	ea	5317	.
1973	me	0424	ch		
5175	s	6824	th		

It ill becomes him to preach that gospel.

Text 21. (Starting in Column 69).

1731	Hi	3557	si	3537	ru
5175	s	3593	to	5151	m
1971	ma	3539	ry	7175	is
3531	ri	7319	of	3519	re
3575	ta	3553	se	1957	lu
5139	l	0462	cr	0468	ct
0262	br	5979	et	5757	an
1531	ea	5175	s	5179	t
6468	st	8224	wh	3593	to
7175	is	7115	ic	5717	ad
5395	the	5119	h	1517	du
3519	re	1397	de	1373	ce
3173	po	1379	co	5317	.

His marital breast is the repository of secrets which decorum is reluctant to adduce.

THE INDICATOR SYSTEM

(i) Starting-point Indicator.

In any message this Indicator is governed by the last 2 digits of the first enciphered group. The Subtractor group in the column indicated by these two digits is set down, and to its first 2 digits and its last 2 digits is added the number of the column in which the message starts. The group thus formed is the Indicator, and is inserted in the text as the second group.

e.g. In Text 1, the first enciphered group is 0866. The Subtractor group indicated by the last 2 digits (66) is 3908. The text starts in column 06, and when this number is added to the first 2 digits and to the last 2 digits of 3908, we have as the Indicator 3504.

(ii) Finishing-point Indicator.

The method of evolving this Indicator is the same as the method adopted for the starting-point Indicator with certain modifications:- It is the first 2 digits of the last enciphered group which determine the Subtractor group, and to this group is added the number of the column in which the message ends. The Indicator thus formed is inserted immediately in front of the final group of the message.

e.g. In Text 1, the last enciphered group is 0888. The Subtractor group indicated by the first 2 digits (08) is 2362. The text ends in Column 65, and when this number is added to the first 2 digits and to the last 2 digits of 2362, we have as the Indicator 8827.