

# CONTENTS

Sections		Page
1.	General Explanation	3
2.	The Right Hand Wheel	5
3.	Wheel Squares	7
4.	Useful Aspect of a Cyphered Message	7
5.	Solution	13
6.	Particular Solutions I When the wheels are known	15
7.	Rectangles	23
8.	Particular Solution II When the wheels are not known	27
9.	General Remarks	36

Figures.	Fig. 1.	page 2
	Fig. 2.	" 30
	Fig. 3.	4
	Fig. 4.	} End of book
	Fig. 5.	
	Fig. 6.	
	Fig. 7.	Loose Sheet No 1.
	Fig. 8.	" " No 2.
	Fig. 9.	page 12.
	Fig. 10.	Loose Sheet No 3.
	Fig. 11.	" " No 4.
	Fig. 12.	" " No 5.
	Fig. 13.	" " No 6.
	Fig. 14.	" " No 7.
	Fig. 15.	page 26
	Fig. 16.	" 26.
	Fig. 17.	" 28
	Fig. 18.	Loose Sheet No 8

Sections		Page
1.	General Explanation	3
2.	The Right Hand Wheel	5
3.	Wheel Squares	7
4.	Useful Aspect of a Cyphered Message	7
5.	Solution	13
6.	Particular Solutions I When the wheels are known	15
7.	Rectangles	23
8.	Particular Solution II When the wheels are not known	27
9.	General Remarks	36

Figures		Page
Fig. 1.		page 2
Fig. 2.		" 30
Fig. 3.		4
Fig. 4.	}	End of book
Fig. 5.		
Fig. 6.		
Fig. 7.		Loose Sheet No 1
Fig. 8.		" " No 2
Fig. 9.		page 12
Fig. 10.		Loose Sheet No 3
Fig. 11.		" " No 4
Fig. 12.		" " No 5
Fig. 13.		" " No 6
Fig. 14.		" " No 7
Fig. 15.		page 26
Fig. 16.		" 26
Fig. 17.		" 28
Fig. 18.		Loose Sheet No 8
Fig. 19.		page 32
Fig. 20.		Loose Sheet No 9

# The Reciprocal Enigma.

## General Explanation.

1. (a) The cyphering is done by 26 Keys, 26 lights and 4 wheels.
  - (b) Three of the wheels are ~~one~~ thorough fares and the fourth causes a return. (see fig 2). at end of book.
  - (c) In figure 2. each strip represents a wheel. The numbers indicate the connections. Thus the 1 on the right hand side of the wheel is connected electrically with the 1 on the ~~right~~ <sup>left</sup> hand side. In wheel IV the 1 is connected with the <sup>other</sup> 1 on the same side etc.  
If the setting of the wheels (given by the numbers on the left-hand side) is 8, 17, 22, 23 & their order IV III I II, then I becomes T. ie if the Key I be pressed the light T shines or if the Key T be pressed the light I shines (see fig 1).
  - (d) When a Key is pressed, first the right hand wheel is moved round one place and then the electrical connection is made. Thus if the setting were III, II, I, II; 8, 17, 22, 22 and the Key I ~~were~~ pressed. first the wheel II would move from position 22 to 23 & then light T would shine.
  - <sup>+</sup>(e) When any wheel comes into position 1 the wheel on the left is at the same ~~time moved up one~~ time moved up one place. Thus with setting IV, III, I, II 8, 17, 22, 26 the Key T is pressed. This moves II to position 1 & I to position 23 & the light Z shines. Similarly with the next wheel. Wheel IV, however, is never [moved by the Keys]
  - (f) The wheels I, II, III can be put on in any order.
  - (g) All the wheels have tyres ~~with~~ marked with letters which can take

(b) Three of the wheels are ~~are~~ through fares and the fourth causes a return. (see fig 2) at end of book.

(c) In figure 2, each strip represents a wheel. The numbers indicate the connections. Thus the 1 on the right hand side of the wheel is connected electrically with the 1 on the ~~right~~<sup>left</sup> hand side. In wheel IV the 1 is connected with the ~~1~~<sup>other</sup> 1 on the same side etc.

If the setting of the wheels (given by the numbers on the left-hand side) is 8, 17, 22, 23 & their order IV III I II, then I becomes T. ie if the Key I be pressed the light T shines or if the Key T be pressed the light I shines (see fig 1).

(d) When a Key is pressed, first the right hand wheel is moved round one place and then the electrical connection is made. Thus if the setting were III, III, I, II; 8, 17, 22, 22 and the Key I ~~where~~ pressed, first the wheel II would move from position 22 to 23 & then light T would shine.

<sup>x</sup>(e) When any wheel comes into position 1 the wheel on the left is at the same ~~time moved up one~~ time moved up one place. Thus with setting IV, III, I, II 8, 17, 22, 26 the Key T is pressed. This moves II to position 1 & I to position 23 & the light Z shines. Similarly with the next wheel. Wheel IV, however, is never

[moved by the Keys.]  
(f) The wheels I, II, III can be put on in any order.

(g) All the wheels have tyres ~~with~~ marked with letters which can take up any position relative to the wheels. The Primary Setting is

II

1	19
2	12
3	22
4	7
5	2
6	20
7	6
8	24
9	10
10	17
11	15
12	8
13	5
14	23
15	9

8	11	2	13	1	19	1	Q	1
11	2	13	3	2	20	13	W	2
13	12	3	5	3	21	11	E	3
2	5	4	10	4	22	16	R	4
10	8	7	12	5	23	3	T	5
1	13	9	7	6	24	14	Z	6
12	6	4	1	7	25	4	U	7
5	3	10	1	8	26	21	I	8
13	7	6	9	9	27	19	O	9
3	4	7	5	10	28	12	A	10
2	6	1	2	11	29	22	S	11
7	3	5	11	12	30	7	D	12
8	2	10	8	13	31	2	F	13
11	9	8	13	14	32	20	G	14
9	13	1	9	15	33	6	H	15
12	11	5	6	16	34	24	J	16
9	4	12	7	17	35	10	K	17
3	1	12	4	18	36	17	P	18
4	10	6	3	19	37	15	Y	19
6	12	13	10	20	38	8	X	20
10	5	3	4	21	39	5	C	21
6	9	8	6	22	40	23	V	22
7	10	11	2	23	41	9	B	23
4	7	9	12	24	42	18	N	24
5	1	2	11	25	43	26	M	25
1	8	11	8	26	44	25	L	26

Pairs given by setting IV, III, I, II 8, 17, 22, -.

Pairs given by setting IV, III, I, II 8, 17, 23, -.

Pairs given by setting IV, III, I, II 8, 17, 24, -.

consists of the setting of these Tyres. Thus suppose the

Primary Setting were IV, III, I, II, MBAP. The wheels

would be put on in the order indicated and the tyres fixed to the wheels so that in IV the M on the tyre was over the 1 on the wheel, in III the B on the tyre was over the 1 on the wheel etc.

(h) The Secondary Setting refers to the letters on the tyre opposite the red line in figure 2. e.g:- Secondary Setting:- TRVK.

When M is opposite 1, T is opposite 8 when B is opposite 1 R is opposite 17  
When A is opposite 2, V is opposite 22 when P is opposite 1 K is opposite 22.

So Primary Setting MBAP; Secondary setting TRVK means that the actual setting is 8, 17, 22, 22.

(i) The Primary Setting could be used for a period of time and the Secondary Setting could be different for each message and sent with it.

The Right Hand Wheel.

2. (a) One aspect of the method is given below.

(h) Consider only the right hand wheel as in the figure 3<sub>A</sub>, and consider the remaining wheels in a lump. The coloured columns of figures give the pairs caused by wheels IV III I in the positions indicated. It is sometimes convenient to think of the right hand wheel moving against a system of pairs for 26 letters & then "switched" over to another system of pairs.

(c) A Message with primary setting MBAP (IV III I II) & secondary setting TRVK

could be cyphered with the wheel II moving from 23 to 26 against the violet pairs

## Particular Solutions I.

- 6 (a) Given (1) The general idea of the machine with the order of letters Q W E R ~~T~~ U etc.
- (2) The connections in the wheels,
- (3) A cypher message.
- (4) The first 15 letters of the clear message "SITUATION REPORT"
- (5) The secondary setting. KCSI which was sent with the cypher message in distinguishable form.

- Find. (1) The rest of the message.
- (2) The primary setting.

(b) First tabulate the cypher message and the first fifteen letters of the clear message as was done in figure 8. (fig 10) Loose Sheet No 3

(c) Make a list of the ~~pairs~~ and first fifteen pairs as in 4(g) (p.9)

1.  $a+1, d+1$
2.  $a+2, d+2$
3.  $i+3, m+3$
4.  $o+4, s+4$
5.  $h+5, v+5$
6.  $s+6, b+6$
7.  $h+7, u+7$
8.  $w+8, k+8$
9.  $u+9, c+9$
10.  $o+10, g+10$
11.  $o+11, g+11$
12.  $r+12, p+12$
13.  $v+13, n+13$
14.  $a+14, b+14$
15.  $x+15, m+15$

(d) Assume that the right hand wheel is I and that the first letter is cyphered with it in the position 1. Substitute for the letters the values given by the 1<sup>st</sup> column in fig 9 starting at the 26<sup>th</sup> line: i.e.  $q=3$   $w=14$  etc.

- We get the pairs.
1. 26, 10
  2. 23, 11
  3. 21, 19
  4. 3, 15
  5. 7, 17
  6. 17, 23

6. conflicts with 5. + 2.  $\therefore$  The assumption made

(p) The correct assumption is that Wheel II is in position 22 & Wheel IV in position 6. ~~is. The pair~~

(q) The secondary setting was KCSI. The actual setting is 6, 22, 9, 5.

∴ The primary setting was F H K E, IV II I III.

### Rectangles

7. (a) Before proceeding to the reconstruction of the wheels from a crib, it is necessary to say something about rectangles.

(b) There are two in figure 8 and one in figure 10. In the former figure ~~if we joined~~ the pairs 2 & 3 to ~~each other~~ are at the corners of a rectangle whose length measured horizontally is one unit. The pairs ~~26~~ 7 & 26 are at the corners of a rectangle of length 19 units. In the latter figure the pairs 10 & 11 form a rectangle of length one unit.

(c) When two pairs form a rectangle ① They must have the same range ② The number of units in the length of the rectangle must equal the difference between the values of the pairs (+ a multiple of 26.)

(d) For example in figure 8. The pairs 2 & 3 are respectively valued at 25, 12 & 26, 13. They have the same range & the ~~length~~ number of units in the length of the rectangle is equal to the difference between the values of the pairs. The pairs ~~27~~ 7 & 26 are respectively valued at 26, 3 and 19, 22. The same remark applies to this rectangle.

(e) Suppose in figure 8, instead of pairs 8, 39, 13, 44, 11, we had had pairs a, b, c, d & e. It will be seen that the pairs a & b, c & d, e & 42

Primary setting IV III I II MBAP.

	5	10	15	20	25	30
q			e	20	21	
w	4					30
e			16	20		f
r					25	
t			18		23	29
z	1	4	6	8	19	
u			8			
i			8	10		
o	1					31
a		5	7			26
s		5				
d				16	24	30
f	2, 3		11 12	19		29
g			14			27 f
h						28
j						
k		9	13 14			
p			13		22	
y		10	11	15		
x						
c		6		15		27
v				18		
b		7	12			25 26 28
n					24	
m				17	21 22 23	
l	2, 3	9	e	17		31

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

Secondary setting TRVK.

Clear I S A W T H E M I N I S T E R F O R F O R E I G N A F F A I R

Cypher T N B N Z L J L K O W Q R L Z V I F X U Z V W L T B X C W N C

Cyphered with wheels IV III I in position TRV.

" " " " " in position TRW.

" " " " " in position TRX.

- 8 (a) Given ① The general idea of the machine with the order of letters QWERTZUVE  
 ② A cypher message with a crib of 180 letters.  
 ③ The secondary setting, sent in distinguishable form.

Find ① The 'relative values' of the connections in the wheels.  
 ② The primary setting.

- (b) In the message given only the 'relative values' of the connections of only the two right hand wheels can be found and the primary setting only of the right hand wheel.
- (c) The message and crib are tabulated on loose sheet No 6 and the values of the pairs on loose sheet No 7. (Figures 13 + 14 respectively)
- (d) In figure 13 the rectangles are indicated.
- (e) In figure 15 are entered the rectangles that might possess an inherent likeness. N.B. If the "switch" occurs between the first pairs or between the second pairs of rectangles then there can be no 'inherent' likeness. The converse of this is not true.
- (f) From figure 16 we can say that switch probably occurs at 12/13, 13/14, 14/15 or 16/17 and that the likenesses of ② + ③ are least likely to be inherent.

(g) Consider ⑥ + ⑤ in Fig 15. if in ⑥  $o-e = k-l = 19$ . Then in ⑤  $o-l = k-e = 4$ . from ⑥ we get  ~~$o-e + k-l = 38$~~  by adding  $o-e + k-l = 38$  + from ⑤  $o-l + k-e = 8$  which conflict. Similarly if in ⑤ we started with  $o-l = k-e = 19$  we should reach the same contradiction.

at 12/13 only one set pair of rectangles [to wit ③] needs to have only a fortuitous likeness

	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	26	II
Q	19	11	20	4	24	15	26	17	2	8	5	23	19	10	21	3	10	8	9	20	17	21	7	17	6	22	Q
W	12	21	5	25	16	1	18	3	9	6	24	20	11	22	4	11	9	10	2	18	22	8	18	7	23	20	W
E	22	6	26	17	2	19	4	10	7	25	21	12	23	5	12	10	11	22	19	23	9	19	8	24	21	13	E
R	7	1	18	3	20	5	11	8	26	22	13	24	6	13	11	12	23	20	24	10	20	9	25	22	14	23	R
T	2	19	4	21	6	12	9	1	23	14	25	7	14	12	13	24	21	25	11	21	10	22	23	15	24	8	T
Z	20	5	22	7	13	10	2	24	15	26	8	15	13	14	25	22	26	12	22	11	1	24	16	25	9	3	Z
U	6	23	8	14	11	3	25	16	1	9	16	14	15	26	23	1	13	23	12	2	25	17	26	10	4	21	U
I	24	9	15	12	4	26	17	2	10	17	15	16	1	24	2	14	24	13	3	26	18	1	11	5	22	7	I
O	10	16	13	5	1	18	3	11	18	16	17	2	25	3	15	25	14	4	1	19	2	12	6	23	8	25	O
A	17	14	6	2	19	4	12	19	17	18	3	26	4	16	26	15	5	2	20	3	13	7	24	9	26	11	A
S	15	7	3	20	5	13	20	18	19	4	1	5	17	1	16	6	3	21	4	14	8	25	10	1	12	18	S
D	8	4	2	6	14	21	19	20	5	2	6	18	2	17	7	4	22	5	15	9	26	11	2	13	19	16	D
F	5	22	7	15	22	20	21	6	3	7	19	3	18	8	5	23	6	16	10	1	12	3	14	20	17	9	F
G	23	8	16	23	21	22	7	4	8	20	4	19	9	6	24	7	17	11	2	13	4	15	24	18	10	6	G
H	9	17	24	22	23	8	5	9	21	5	20	10	7	25	8	18	12	3	14	5	16	22	19	11	7	24	H
J	18	25	23	24	9	6	10	22	6	21	11	8	26	9	19	13	4	15	6	17	23	20	12	8	25	10	J
K	26	24	25	10	7	11	23	7	22	12	9	1	10	20	14	5	16	7	18	24	21	13	9	26	11	19	K
P	25	26	11	8	12	24	8	23	13	10	2	11	21	15	6	17	8	19	25	22	14	10	1	12	20	1	P
Y	1	12	9	13	25	9	24	14	11	3	12	22	16	7	18	9	20	26	23	15	11	2	13	21	2	26	Y
X	13	10	14	26	16	25	15	12	4	13	23	17	8	19	10	21	1	24	16	12	3	14	22	3	1	2	X
C	11	15	1	11	26	16	13	5	14	24	18	9	20	11	22	2	25	17	13	4	15	23	4	2	3	14	C
V	16	2	12	1	17	14	6	15	25	19	10	21	12	23	3	26	18	14	5	16	24	5	3	4	15	12	V
B	3	13	2	18	15	7	16	26	20	11	22	13	24	4	1	19	15	6	17	25	6	4	5	16	13	17	B
N	14	3	19	16	8	17	1	21	12	23	14	25	5	2	20	16	7	18	26	7	5	6	17	14	18	4	N
M	4	20	17	9	18	2	22	13	24	15	26	6	3	21	17	8	19	1	8	6	7	18	15	19	5	15	M
L	21	18	10	19	3	23	14	25	16	1	7	4	22	18	9	20	2	9	7	8	19	16	20	6	16	5	L

Fig. 5.

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 26